Classifying high performance computing system breaches and finding common trends

by

ZINTLE SANDA

Thesis submitted in fulfilment of the requirements for the degree:

MTech: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Prof M Weideman

Co-Supervisor: Ms Tabisa Ncubukezi

Cape Town

Date submitted: 5 December 2023

DECLARATION

I, Zintle Sanda, declare that the contents of this thesis represent my own unaided work and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

STUDENT:

.....
Signed

4 December 2023
.....
Date

SUPERVISOR:

.....
Signed

4 - Dec - 2023
.....
Date

ABSTRACT

The remarkable growth of cyber connectivity and remotely delivered services has resulted in cybersecurity taking priority among other challenges. High Performance Computing (HPC) facilities are subject to the same styles of attacks, as they have an active internet connection and run the same as any other computer. Efficiently securing an HPC system that needs to be convenient and open to its users, comes with security vulnerabilities and challenges to balance the two. Traditional security solutions do not perform well with HPC systems as they can affect performance. Recent attacks have been taking advantage of security weaknesses in hardware design. It is paramount to build security within the solution during design, rather than as an add-on or afterthought.
There remains a lack of a classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.

A literature survey was done, and it was found that major concerns of security on HPC systems are not only on the software side but also on the hardware. Security through system hardware helps protect against vulnerabilities exploited from the software level. Writing better applications to try to fix hardware-based security flaws is not actually addressing the underlying architectural flaws.
As HPC processor speeds are increasing, numerous threats have emerged and seem to be developing even more quickly because of it. Most of these vulnerabilities are related to how contemporary CPUs use cache and speculative execution. They may be able to grant unauthorised access to confidential data and can affect processor performance. Literature also shows that there are interferences affecting several conventional memories at the circuit-level, that can be hardware vulnerability aiming to gain privilege escalation, cause denial-of-service or leak sensitive data.
The trade-off between performance and computer security has been an important computer development consideration throughout the years. The literature shows that the future of security is at the hardware level. Past security approaches of “just enough security” on systems have shown various security gaps because the hardware was optimised for speed and never for security.
Several cyber countermeasures on detecting attacks have been implemented such as operating system (OS) modification and data execution prevention. The use of hardware counters built-in

modern microprocessors is becoming a prominent approach and hardware that is not trustworthy is a disastrous loss of security.
It is desired during runtime that firmware security systems provide protection, detection, and restoration. This safety would preferably extend to peripheral parts and motherboards central processing unit (CPU) running firmware.
The research aims to adopt the survey research for data collection and to analyse and interpret it adopting descriptive statistics, specifically utilising convenience sampling as determined by the researcher. It will be looking into the risks involved in hardware security, such as the type of attacks that target the hardware of a system designed to operate in a HPC environment and their impact if these hardware systems are not secured.

RESULTS

It is anticipated that the study's conclusion will confirm the common trends of malware attacks that are targeting HPC systems hardware **It is also expected to work towards finding the best way to create a defence mechanism for hardware designs.**

CONCLUSION

In conclusion, it is expected to find that there are benefits of adapting security during design. Any programmer or engineer designer working on new systems intended to be used in an HPC environment should consider the security in design mechanism to limit the security causing impact in the system performance.

Key words: high performance computing (HPC), security, malware, performance, hardware

ACKNOWLEDGEMENTS

I wish to thank:

▪ God, throughout my research journey.

▪ I would also like to extend my gratitude to my family and friends who supported me throughout the duration of my study.

▪ My supervisor, Prof Melius Weideman, for his diligent responsiveness, guidance, and encouragement during this journey.

The financial assistance of CSIR towards this research is acknowledged. Opinions expressed in this thesis and the conclusions arrived at, are those of the author, and are not necessarily to be attributed to the CSIR.

DEDICATION

This study is dedicated to my son, Ngazibini Sanda. I hope this encourages you to always aim to do your best in everything you do.

ABBREVIATIONS AND GLOSSARY

ACRONYMS

Glossary	Acronyms
HPC	High Performance Computing
UEFI	Unified Extensible Firmware Interface
I/O	Input / Output
DDoS	Distributed Denial of Service
PKI	Private Key Infrastructure
SIAM	Service Integration and Management
OS	Operating System
CPU	Central Processing Unit
SCSI	Small Computer System Interface
CHPC	Centre for High Performance Computing

GLOSSARY

Terms	Definitions/Explanation
High Performance Computing	The use of high performing computers or supercomputers that use parallel techniques to solve complex calculations (Sadiku, Sarhan, & Osama, 2017).
Security	Protection against a cyber-attack towards theft of e-data or damage of the hardware and software (Pittalia, 2015).

System	A set of interconnected computers that work together as part of one big powerful computer (Buyya, 1999).
Performance	The amount of computational work that can be accomplished by a system (Kocher et al., 2018).
Computing	A technique of processing complex calculations (Sadiku et al., 2017).
Resources	The components that perform the computing in the system, such as CPU (Al-Jody et al., 2020).
Firmware	Permanent programmed software in read-only memory (Khessib et al., 2019).
Hardware	Machine, wiring and other electronic systems physical parts (Basu et al., 2020).
Operating system	Software that controls a computer's software and hardware resources and provides access to application computer programs (Yellu et al., 2019).
Malware	Software intended specifically for disrupting. Damaging or gaining unauthorised access to a computer system (Alves & Morris, 2018).

TABLE OF CONTENTS

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

CHAPTER FOUR: RESULTS AND ANALYSIS

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE: BACKGROUND AND RESEARCH PROBLEM

1.1 INTRODUCTION

The remarkable growth of cyber connectivity and remotely delivered services has resulted in cybersecurity taking priority among other challenges. These cyber threat challenges have necessitated proactive and dynamic solutions (Maitra & Madan, 2017). Cybersecurity is a key component of all computing techniques and Peisert (2017) states that High Performance Computing (HPC) facilities are subject to the same styles of attacks, as they have an active internet connection and run the same as any other computer. HPC refers to the use of high performing computers or supercomputers that use parallel processing techniques to solve complex calculations (Sadikual et al., 2017). Systems with a wide variety of designs, configurations, and technologies are referred to as high-performance computing (HPC) systems. Their purpose is to provide high computational performance and throughput for workloads that are demanding (Sadikual et al., 2017). Supercomputing systems like distributed memory systems (such as hybrid systems and clusters), shared memory systems (such as symmetric multi-processors), vector computers and huge parallel processors, are among several types where these system categories are determined by their architectural design (Mabakane, 2019).

This research will focus on cluster systems which are widely used in academic, research, and industrial settings to tackle computationally intensive problems across various disciplines and domains, Kamila et al (2021). A cluster is a group of computers (nodes) linked through a network and operating as an integrated single computing resource (Mabakane, 2019). Clusters are built from the same basic hardware as the desktop PC, although their computational capabilities are more powerful than those of a desktop.

A cluster consists of different components that make the system function as one; firstly it consists of a head node that is used for user access to submit programs, then a management server used to store images such as an OS that can be distributed to compute nodes, it also consists of a resource manager that is responsible for allocating resources to the submitted programs, and then it consists of compute nodes that perform the processing. There is also a parallel file system connected to these compute nodes for I/O functions, it has its own server to manage the file system and store data paths. There are also secondary servers that perform the retrieve and write functions of the file system. The management server has access to every other component on the cluster system and compromise on it, compromises the whole system.

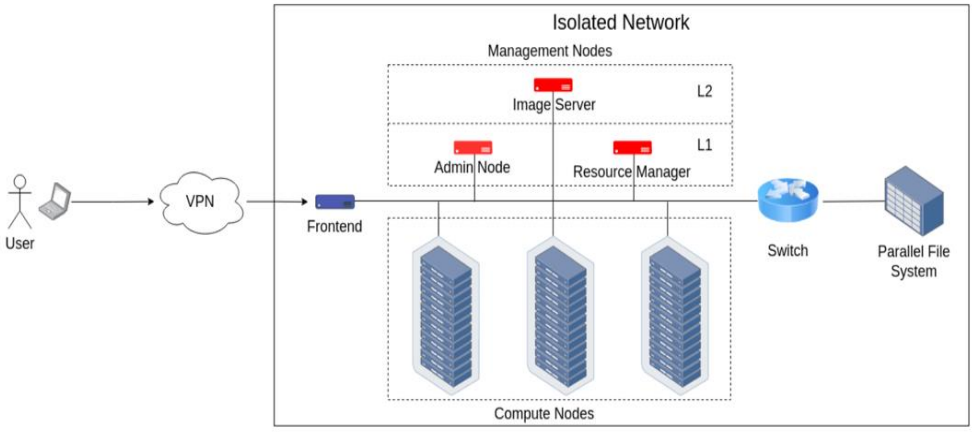

Figure 1.1: A typical drawing of an HPC system
Nolte et al. (2022)

A perimeter firewall is usually in place to safeguard HPC systems, and jump hosts are the only way to access them.

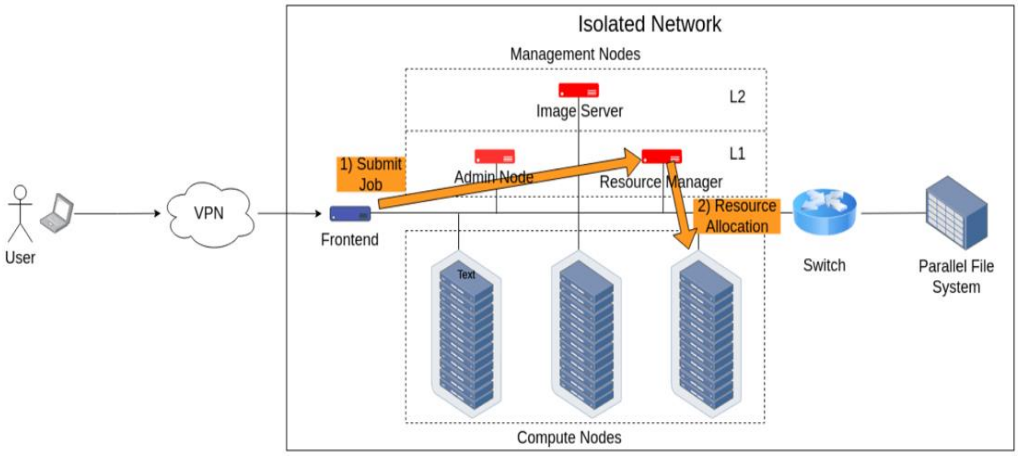

Figure 1.2: A drawing of a typical workflow for users on an HPC system Nolte et al. (2022)

HPC cluster systems was chosen as it is the common system used by academia in the SADC country universities.
Attacks such as compromised user credentials to get access to their accounts and data, brute force login attempts, and scans are vulnerabilities that still cause problems for HPC systems.
HPC systems resources also can perform attacks on other systems, like to launch a DDoS attack, where the perpetrator seeks to make a machine or network unavailable, thus consuming system resources required by authorized users.

Securing a system that also needs to be convenient and open to its users, brings vulnerabilities and challenges where intrusion prevention is concerned (Sadiku *et al*, 2017). Zakhour (2017) states that traditional security solutions do not perform well with HPC systems, as they can affect the performance or end up blocking legitimate data transfers.

Computing time on HPC systems is one of the vital assets of its purpose and historically, security is not different from general computer security, other than making sure it does not interrupt HPC system performance or usability (Peisert, 2017).
Spalazzi and Vigano (2015) found that balancing HPC and Security is a challenging task because adding security measures tends to

degrade performance and solutions that seem to impose on computing time bring reluctance to an agreement.

To be able to identify adequate security requirements, Ansari et al (2018), found that these requirements are key aspects of engineering a secure system. These security requirements also compete with cost and usability, making it a challenge to provide complete security. Trading-off security against these other requirements is partially satisfied to achieve “good enough security”.

There has been a growing demand for HPC services, due to researchers requiring more resources. HPC workloads have increased and become more compute-intensive, demanding a shift to cloud computing where resources are unlimited compared to in-house HPC running at capacity (Burt, 2017).

With the advantages that cloud computing is bringing, there are still concerns with reliability, such as security (Varghese & Buyya, 2017).

According to Wayhmare and Kapse (2015), cloud computing was primarily designed to provide services through distributed or virtualized machine technology on demand.
In the last decade, the provided services in cloud computing have rapidly changed due to industry and academia realizing computing as a utility (Varghese & Buyya, 2017).

1.1.1 BACKGROUND TO THE RESEARCH PROBLEM

Science is changing the way things are done as HPC is evolving, both improving its security and bringing more complications. Maitra and Madan (2017) state that with the rapid growth and change in the way science and research is being done, HPC systems are becoming increasingly used to deal with these changes efficiently

and effectively. This has brought more security challenges in how data is protected (Peisert, 2017).

According to Bulusu et al (2018), there is still a belief that HPC security is in parity with traditional security. The capacity in which HPC systems can perform is attracting more hackers that want to exploit any security vulnerability for their gain to use these weaknesses to perform other cyber-attacks, such as DDoS attacks. The authors believe that the security of HPC infrastructure is more complex compared to the infrastructure of traditional data centres, yet when it comes to security HPC systems are treated as a collection of independent machines instead of a single unit.

The relationship between HPC and security has a vital influence on the types of security solutions that can be acceptable to use in the HPC community. Adding security measures typically degrade performance, making it a challenge to balance maintaining high performance and achieving security. To have an open HPC environment presents an HPC challenge to security and traditional security solutions are often not effective (Peisert, 2017). Fernandez-Gonzalez et al. (2015), suggest that the design of communication networks for data exchange among system nodes is still an issue requiring new ideas.
Due to degraded performance issues, security solutions that mostly detract from computing time bring reluctance to use these solutions; thus, these systems cannot resist common attacks due to the security support being poor. When it comes to the security of HPC systems, research was done on the software level, while hardware security has been invested-on less. (Fargo & Sury, 2018).

This research will be looking at the security of the Unified Extensible Firmware Interface (UEFI) and BIOS, as this is the crucial initialization of computer hardware, in the case of HPC systems (a management server). It is hard to identify or remove

malicious software that has managed to compromise the UEFI, thus compromising the whole cluster system.

Therefore, the research problem for this research project is: **There is a lack of classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.**

1.1.2 OBJECTIVE and RESEARCH QUESTIONS

Research Problem	There is a lack of classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.

Research Objective	**Research Questions**
To contribute to guidelines towards the design of a security mechanism that can be used to prevent threats in HPC systems.	1. What are the vulnerabilities in an HPC environment? 2. How can these vulnerabilities affect HPC systems? 3. What types of threats these vulnerabilities attracted to HPC systems in the past? 4. What could a potential solution to this problem look like?

Table 1.1: Summary of Research Problem and Objectives

1.1.3 PURPOSE OF THE STUDY

Outcomes: This study will be contributing towards a framework development that classifies hardware security breaches in HPC systems for understanding, prioritising, and mitigating threats, thereby enhancing the resilience and security posture of HPC environments against malicious attacks.

Contribution: By addressing the uncertainty surrounding where to focus protection efforts, the research contributes to strengthening the resilience and security posture of HPC environments against malicious attacks.

Significance: A standardised classification framework serves as a valuable resource for researchers as the significance of resolving the research problem lies in its potential to strengthen the security, resilience, and trustworthiness of HPC systems. This fosters the development of innovative solutions, technologies, and methodologies for protecting HPC systems against emerging threats.

1.1.4 RESEARCH DESIGN and METHODOLOGY

According to Bredford (2017), deductive reasoning starts with a general statement and discusses the possibilities for drawing a specific logical conclusion, while inductive reasoning generalises broadly from observations, then conclusions are drawn from that. This research will adopt the non-probability sampling method. It will be a convenience sample, where the population of this study's audience is humans working on HPC systems and security administrators whose email addresses the researcher has.
This research will be using deductive reasoning, where it will be looking at patterns of security attacks targeting hardware of a system, analyse and interpret those trends by generalising the findings to get a conclusion.

According to Bennett and McWhorter (2016), quantitative research focuses on inference, the development of new hypotheses, and the discovery of phenomena.
This research aims to recognise and test the theory by adapting the quantitative method. It will be looking into the risks involved in hardware security, such as the type of attacks that target the hardware of a system designed to operate in an HPC environment

and their impact if these hardware systems are not secured. This research will be limited to malware attacks targeting firmware of system hardware and finding common trends. It will work towards finding the best way to create a defence mechanism.

1.1.5 DELINEATION OF THE RESEARCH

The study will be conducted at an institution with an HPC system (cluster). This study will involve some of the systems administrators who administer the system to conduct the research. It will not cover all research in HPC security, neither the security of a computer lab, a standalone server, or a single computer but will only focus on the security threats targeting an HPC system hardware.

1.1.6 OVERVIEW of the CHAPTERS

- **Chapter 1:** The study's research design and methodology are explained in this chapter. The historical context was the subject of the introductory literature review in HPC, the research topic, goal, objectives, and delineation are all included in the general introduction.
- **Chapter 2**: In this chapter, previous related studies are explored and a review of the HPC and security literature is presented.
- **Chapter 3:** The tools and methods for data collection and analysis are discussed in this chapter.
- **Chapter 4:** This chapter covers the results and findings of the data collected for the research. The themes of the research questions are examined in depth in this chapter.
- **Chapter 5:** Based on the data analysis, a conclusion was reached, and recommendations of the research are covered here.

1.1.7 CHAPTER SUMMARY

This chapter explored the topic of classifying high performance computing system breaches and finding common trends. The chapter began with a background of the problem and the research problem, followed by a discussion of the research questions and

the research objective. The research methodology and research delineation were also stated and, finally, an outline of the thesis structure was presented. A literature review on the thesis topic will be undertaken in the following chapter.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

HPC and Security are two broad topics that research can be focused on. This research will focus on the currently available literature for the given topic area focusing on HPC security, cloud computing, cybersecurity, and cyberattacks.

2.2 HIGH PERFORMANCE COMPUTING

High Performance Computing refers to the use of high performing computers or supercomputers that use parallel processing techniques to solve complex calculations. These supercomputers allow users (researchers) to solve complex and compute-intensive problems in science (Sadiku, Sarhan & Osama, 2017).

According to Sadiku et al (2017), a cluster is one of the popular examples of what an HPC system is. A cluster refers to a set of computers connected to a network, working as if it is one big computer. HPC systems were originally designed to perform many calculations in a short period of time (Peisert, 2017). González et al. (2015), state that HPCs were originally designed for military use only with limited network communication. Peisert (2017) found that data analysis is also an element added to the purpose of HPCs today.

According to Al-Jody et al (2020), whether on-premises or in the cloud, the two most frequent techniques to deploy HPC parallelism are computer clusters and grids.

These systems have different purposes or uses and have a distinctive way to carry out their purpose, though they are distinctive systems, they seem to have a regular or predictable way of operating which challenges the way security can be enforced.

HPC systems tend to be more open to security threats, with users who use those systems, accessing them with invalidated information (Peisert, 2017). According to Peisert and Sadiku et al (2017), the main concern for users (researchers) is diminishing the purpose of HPC by wasting cycles due to security solutions imposing on computing time.

Peisert (2017) found that understanding the core purpose of the HPC system enables one to establish solutions for security policies and determine how to enforce them.

Applications for HPC are designed to mirror the parallel architecture of HPC systems. Software development, parallel algorithms, and HPC system architecture are the main areas of current studies, Nolte et al (2023).

According to Al-Jody et al (2020), there have been no substantial efforts to define standardised security standards for HPC systems. On a fundamental level, HPC security standards exist, such as Private Key Infrastructure (PKI) on the system's edge, and they are assumed to be sufficient.

According to Al-Jody et al (2020), the management of resources and users in HPC systems is frequently added to or incorporated into existing security policies at the institution that fail to account for the diversity of HPC systems and extra cyber security requirements**.** Nolte et al (2023), the user's terminals or portals for accessing High Performance Computing resources are often insecure or connected to unprotected networks.

The authors state that there are various challenges in HPC, these systems are frequently protected by institutional firewalls, and each institution has its own policy, which the e-science certificate authority checks on a regular basis. To gain access to HPC resources, most registered users use SSH (secure shell).

Many HPC centres now use Private Key Infrastructure (PKI) as a core form of authentication and authorisation because it is reliable. However, even with PKI authentication in place, users with a poor level of security awareness face security threats. Most cyber-attacks follow a predictable pattern, with tell-tale signs that they're progressing, but they're typically hard for HPC system administrators to discover, Al-Jody et al (2020).

The author believes that there is an effort to develop technologies like Security information and event management (SIEM), that will aid administrators in detecting threats. SIEM collects events and data from almost all computer system components, resulting in a tremendous amount of data that administrators have challenges handling in real-time. As a result, when planning and developing such systems, several considerations must be made.

In HPC systems according to Nolte et al (2023), robust and secure access protocols must be built as the number of threats is increasing. Nolte et al (2023), finds that, it is becoming difficult for administrators to adequately manage system security using existing technologies. As the present standards do not give enough data to identify and prevent modern attacks adequately, HPC resources are often accessed behind institutional firewalls, and their users can access them remotely or locally using a variety of systems. The design of contemporary HPC systems is so intricate that it is difficult to estimate the performance of an application. For these systems, iterative optimisation is carried out repeatedly to maximise performance, Al-Jody et al (2020).

According to Nosek et al (2022), modern computer processors help with this by offering hardware performance counters that give low-level access to comprehensive data acquired during code execution.

Users of HPC systems are far more inclined to rely on performance counter results due to the ongoing demand for fast and efficient

code. System administrators are under pressure to enable the performance counters despite the possible security risks this presents.

HPC systems often operate in secure, regulated environments, which helps to lessen the risk. Some of the useful code is created and added from outside of these restricted areas, therefore, it is essential that the performance tools and operating systems running on the untrusted code be resistant to security flaws (Weaver, 2022).

2.3 CLOUD COMPUTING

According to Singh and Chatterjee (2017), cloud computing is the provision of on-demand services over the network, with a lower cost of services for the user. It is a model designed to enable access to a shared collection of computing resources, network connections, storage, and applications (Messerli, Voccio & Hincher, 2017).
Users access these resources via web-based tools or applications as if they are locally installed programs. Most cloud computing infrastructures deliver services through using HPC centres, which appear to a user as a single point of access (Messerli et al., 2017).

The adoption of cloud computing in HPC has become popular within the enterprise and service providers, but HPC users must deal with a different architecture of cloud computing systems such as heterogeneous resources. Heterogeneous resources are systems that use multiple processors or cores. By adding dissimilar processors, these systems gain performance typically by integrating different processing capabilities to handle specific tasks (Sadiku et al., 2017).

According to Messerli et al (2017), cloud computing systems are not the same as bare-metal machines; they differ in the way they deal with the privacy of user data and the control of the hardware

basis. The differences are fourfold, namely: private clouds, public clouds, multi-vendor clouds, and hybrid clouds.

A private cloud is an internal cloud dedicated to a single organisation's needs and goals that can either be managed internally or off-premises. A public cloud consists of an HPC infrastructure publicly available to the general users or a large industrial group, where users can access compute resources owned and maintained by the cloud service company over the internet. A multi-vendor cloud is a multiple cloud deployment such as a mixture of multiple private clouds or public clouds. A hybrid cloud is a composition of both private and public clouds allowing an organization to coordinate workloads across two cloud deployment environments (Messerli et al., 2017).

The transformation from local to remote computing still brings challenges and security issues regardless of the advantage that cloud computing may bring. According to Singh and Chatterjee (2017), the sharing of resources in a cloud environment by multiple users is still the most open security issue regardless of the number of solutions already available. Managing user credentials in the cloud is an example of one of the challenges.

According to Aljumah and Ahanger (2020), cloud computing services can be misused, compromising not only the organisation's sensitive data but also the user’s personal identity and information.

The loss of data is one of the most significant hazards connected with using the cloud. Data can be compromised in a variety of ways, including deleting or changing the original content. In the cloud, the loss of data caused by a virus or malware that affects hardware, backup storage, and data recovery can be disastrous (Alijumah & Ahanger, 2020).

Alijumah and Ahanger (2020), state that cloud computing systems are vulnerable to a variety of assaults and hacking efforts, which

can cause significant damage to cloud computing service providers. Hackers are coming up with new ways to infiltrate highly secure systems through malicious attacks.

2.4 SECURITY

Knowing the fundamental issues and risks surrounding cybersecurity is key to understanding its problems. With computers and the internet having no boundaries, there has been an exponential growth in the possibilities of exploiting systems. Security on HPC systems is a major concern not just on the software side, but also on the hardware side, due to studies showing that users who are malicious and are using the same physical infrastructure as regular users can attack them through hardware (Fargo & Sury, 2018).

Security through system hardware helps protect against vulnerabilities exploited from the software level. Writing better applications to try to fix hardware-based security flaws is not actually addressing the underlying architecture flaws (Jungwirth et al., 2018).

At the software level, challenges imposed by attacks such as DoS, network, and insider attacks, have been studied but largely neglected on the hardware level. Fargo and Surg (2018) stated that current security measures try to apply reactive solutions to these challenges, but in the study conducted, they recommended a solution called moving target defence (MTD). This is a technique for systems to self-defend against attacks. MTD technique has been mostly used to decrease the level of vulnerabilities in systems against attacks by continuously changing the high level of configurations e.g., execution environment, instruction set and network configuration, etc.

The authors found that seamless cybersecurity protection is needed that will prevent and defend against attacks and that solutions of cybersecurity are at the hardware level.
The main goal of an attacker is to exploit weakness by remaining anonymous and taking advantage of the stolen information. Some of the known attacks include malicious code hidden in software (malware) or Trojan horses and they are mostly used to create remote backdoors for attackers. According to Jungwirth et al (2018), recent attacks are taking advantage of security weaknesses in hardware designs.

The trade-off between performance and computer security has been an important computer development consideration throughout the years. The authors found that the future of cybersecurity is at the hardware level. Past security approaches of “just enough security” on systems have shown various security gaps because the hardware was optimized for speed and never for security.
The excessive complex design of hardware to maximize performance has opened more security gaps (Kocher et al., 2018). There have been concerns with software-based security, due to how vulnerable they are to cyber-attacks.

Balancing performance and security in high performance computing systems is a challenge, with the performance of these machines being one of the top requirements, but it is still clear that a secure system is highly desired by its users (Fargo & Sury, 2018).

Several researchers from different disciplines in academia are entrusting their sensitive data to HPC systems. This emphasises the value of a secure HPC infrastructure in disciplines as diverse as disease eradication, biomedical research, and the mining and geological industries. (Yellu et al., 2019). The authors state that escalation attacks, unlike desktop computers, are a substantial threat to HPCs (particularly multi-user HPC systems).

According to Weaver (2022), HPC systems are susceptible to a wide range of security attacks. Tools for performance analysis are a common source of vulnerabilities that are missed.
These authors also found that security flaws in performance measuring interfaces may result in data leaks, DoS attacks, and even system compromise. Disabling performance interfaces on desktop computers can reduce risk, but on HPC systems, where performance is crucial, it isn't always feasible.

2.5 CYBER ATTACKS

Cyber-attacks are malicious or deliberate actions conducted by an organization or individual to disrupt, destroy, or deny access to a computer system (Shamsi et al., 2016). Attackers are increasingly getting more advanced in their ways of compromising computing infrastructure, and cybersecurity is of prime countermeasures to mitigate cyber-attacks (Forman, 2018). There is a growing effort for these cyber-attacks to become persistent while also avoiding detection by targeting low-level hardware components because the OS executes instructions from hardware and if it is difficult to reclaim control of a system once the hardware has been compromised (Alves & Morris, 2018).

According to Forman (2018), Nosek et al (2022), several cyber countermeasures on detecting attacks have been implemented such as the OS modification, by incorporating security enhancements and patches that can strengthen its resilience against known vulnerabilities and exploits.
Another countermeasure is the data execution prevention, where malicious code execution can be prevented by designating specific memory locations as non-executable. This prevents attackers from executing arbitrary code by taking advantage of memory-based vulnerabilities. The use of hardware counters with built-in modern microprocessors is becoming a prominent approach (Zhang et al., 2022).

According to Alves and Morris (2018), hardware that is not trustworthy presents a disastrous loss of security. The implications of malicious code (malware) written for hardware strictly depends on the system architecture and so different device architectures will require code modifications.
System hardware includes several components on the motherboard that execute devoted firmware that instruct the boot-up and low-level runtime control (Khessib, Kelly & Bulusu, 2019). The authors state that firmware safety is essential to the computer hardware platform's integrity. Vectors for firmware attacks include boot and pre-boot, host access, power reset, network access, and virtual machine access. Additional platforms present extra surface for firmware attacks in contemporary data centres, by enabling physical access to a multitude of hardware resources by virtual machines (Khessib et al., 2019).

According to Khessib et al (2019), it is desired during runtime that firmware security systems provide protection, detection, and restoration. This safety would preferably extend to peripheral parts and motherboards central processing unit (CPU) running firmware. Torbet (2019), states that a piece of sophisticated malware and advanced techniques like trojan UEFI rootkit that was developed to target anti-theft software called LoJax, have the capability to get on the UEFI and BIOS when used together. These malicious software tools can spy on UEFI firmware and may even remove system memory in some instances. This allows hackers to install a malicious UEFI update so that they can access the system and spy on the content or make changes. Even when the OS is reinstalled, the malicious software will still function because it lives on the motherboard.

According to Elnaggar et al (2021), trojans, viruses, worms, adware, and Rootkits are just a few examples of malware.

- Trojan horse: malicious programs that pose as trustworthy software to fool users into installing them. Once installed, they can carry out a variety of destructive tasks, including

destroying system files, opening backdoors for remote access, and stealing confidential data.

- Viruses: Self-replicating programs that attach themselves to trustworthy files or applications. They can lead to several negative outcomes, such as data corruption, unstable systems, and illegal access, and they propagate by infecting other files or systems.
- Worms: Stand-alone malware that can spread over networks on its own without human assistance. They propagate quickly and infect a lot of systems in a short amount of time by taking advantage of flaws in software or network protocols. Payloads that can inflict harm or allow remote control over compromised systems are frequently carried by worms.
- Adware: Designed to show users unsolicited adverts or route them to dangerous websites. Usually, it enters computers through misleading advertising techniques or software bundles. Adware can impair system functionality, jeopardise user privacy, and act as a gateway for more malware infestations.
- Rootkit: Programs created to hide their existence and actions on infected systems. They frequently target the kernel or firmware of the operating system, giving attackers continuous access to compromised systems and the ability to keep control over them while avoiding detection by security tools.

Alves and Morris (2018) stated that there are various approaches to sabotage the system through hardware attacks. Some examples of hardware malware attacks although not all are explained below.

2.5.1 The stealth hard-drive backdoor

Hardware-drive backdoors are extremely hardware-dependent, so customization is required for each targeted device. Most hard drives are based on systems-on-chip (SoC) design. The SoC generally has

a core that stores the firmware for the microcontroller with the same RAM, ROM, and flash memory. It is the responsibility of the microcontroller to translate and store the data requested from the Serial ATA (SATA) or the Small Computer System Interface (SCSI) into cache memory (Alves and Morris, 2018).

According to these authors, infected firmware can take advantage of the microcontroller's privileged position and deliberately alter the read or write information to disk plates. The altered firmware does not need physical access to the hard drive. Using the firmware update mechanism of the manufacturer, a single local or remote access with root privileges is sufficient to re-flash the hard disk firmware. It can be done through malware, which temporarily infects the system to reprogram the firmware of the hard disk and then removes itself to stay undetected from the system (Alves & Morris, 2018).

If the firmware on the management server of the parallel file system in a cluster was also compromised, the malware can change the path list where data is stored or also send a write request to alter the data stored on the hard drives.

2.5.2 Exploiting I/O MMU Vulnerability

The notion of virtual memory is implemented by all modern OS with each method running in a distinct address space. This allows isolation of memory so that various OS on the same machine are unable to see each other's address space. The Memory Management Unit (MMU) is a device that is responsible for translating the address from virtual to physical memory. Usually, devices linked to the bus on the motherboard do not have virtualization of memory, instead, they all share the same address space and use Direct Memory Access (DMA) to access physical memory. DMA allows I/O controllers to directly pass data to or from the main memory. This can become a major threat as malicious devices can use this mechanism's advantage to manipulate critical

memory regions such as the kernel of the OS (Alves & Morris, 2018).

The authors stated that I/O MMU was created to increase security by separating the address space of a device; however, it may also contain certain vulnerabilities that may allow malicious code access to protected resources (Alves & Morris, 2018).
If the UEFI is compromised on a management server that manages the whole cluster system, hackers can modify the security of the UEFI and perform functions without security enabled to gain access to the OS kernel to plant the malware.

2.5.3 Printer Firmware Modification

Updating firmware is an omnipresent characteristic found in contemporary embedded devices and the majority do not need authentication to update. According to Alves and Morris (2018), the objective of the firmware modification attack is to inject malware into the device integrated by modifying firmware through an update process.

2.5.4 Malicious Hardware that Enables Software Attacks

According to Alves and Morris (2018), previous attempts were made to create hardware-coded Trojans for the Integrated Circuit (IC) design to leak data. These Trojans are difficult to detect and can only operate at the hardware-level. Their malicious circuit is only functional for a particular purpose and if data at the higher-level abstractions are not mapped to hardware, it makes it difficult for the Trojan to be collected.

2.5.5 Stealing Data with an L3 Cache Side Channel Attack

Modern OS implements the notion of shared pages to decrease the system's memory footprint. Shared pages between two or more processes are identical portions of memory. Usually, the OS

produces location-based shared pages, which is the case with shared libraries (Alves & Morris. 2018).

Shared pages, however, can also be developed by actively searching and combining the same content (deduplication). The OS sets the pages to read-only or copy-on-write to implement isolation, however, some type of inter-process interference is not prevented (Alves & Morris, 2018). Upon touching a shared page, it is copied to the cache of the processor. This cache mechanism can be used by a side-channel attack method to obtain data about shared memory pages access. The method utilises the clflush also known as a cache flush, which is an instruction to clear or invalidate the contents of the cache memory.
In multi-core or multi-processor systems, the cflush or cache flush instruction is a processor instruction that is used to clear or invalidate cache entries, guaranteeing cache coherence and consistency. It aids in preserving synchronisation and data integrity at all memory hierarchy levels (Alves & Morris, 2018).

2.5.6 A malicious USB device

To enhance the connection of plug-and-play devices to PCs, the USB standard was developed, and USB devices are the world's most widely used. The USB Flash Drive is a flash memory with a built-in USB interface (Alves & Morris, 2018).

Due to this, it has become an enormous attack vector for malicious code because of its extensive use. Malware that was developed targeting USB Flash Drives was implemented automatically once the USB is inserted into the computer. The malware also copies to any USB that is inserted into the infected computer. Most anti-malware software prevents the automatic execution of code by USB Mass Storage Devices when inserted, mitigating this attack. However, another attack category can take advantage of USB devices.

The attacker uses the USB to declare itself as one of the devices that follow the Human Interface Devices (HID) specification, making it accepted by the OS without driver installation, for example, keyboards. Therefore, a malicious USB HID device can conduct operations without user interference (Alves & Morris, 2018).

Alves and Morris (2018), believe that although the changes in hardware and firmware from malware attacks are very specific to each device, they have demonstrated to be very effective against software protection. Software completely relies on hardware to conduct its operation, making it difficult to regain system control if the hardware is tampered with (Alves & Morris, 2018).

Sometimes when troubleshooting a certain node on the cluster and cannot do it from the management server, you must physically connect a screen and keyboard to the node (computer) to access it. In this instance, an insider attack can use the advantage of a malicious USB HID device to insert malware on the node. According to Basu et al. (2020) malware can range from simple ads to rootkits that secretly alter kernel control flow. Trusted hardware-based malware detection approaches have recently been created on the basis that software-based defences are easier to overcome than hardware-based counterparts.

These techniques assume that while an attacker may quickly modify software, interfering with hardware is more difficult. Hardware Performance Counters are a type of hardware-based virus detection mechanism inherent in all modern CPUs and used to monitor and fine-tune system performance. (Basu et al., 2020). Basu et al. (2020) also state that malware has been used to disrupt normal computer activity for a variety of reasons, including amusement, notoriety, financial gain, and espionage. This software-based strategy is insufficient, as seen by the constant emergence of new malware.

Researchers have begun to use features embedded in trustworthy devices for malware detection.
The author states that with wide range of security measures, including the firewall, it should be a solution to the security difficulties, intrusion prevention system, anti-virus, rule-based network scanners, and a technique for detecting intrusions that spans multiple layers of a computer system, Nolte et al (2023). However, due to human factors, this is not the case.

Al-Jody et al. (2020) found that for safe access to HPC resources, there are no commonly acknowledged options.
According to Nolte et al. (2022), a safe source system must be the source of trust for a system that is otherwise untrusted. This is because modern software applications heavily depend on open-source software that is accessible to the public and combine packages developed by multiple authors (Gamblin and Katz, 2022). Many security measures, including firewalls, lose their effectiveness after a person has gained access and they may be able to leverage vulnerabilities or exploits to obtain privileged access to the entire HPC system (Mildenberger, 2023).

According to Mildfenberger (2023), after an intruder gains access to a system, several software and hardware vulnerabilities are frequently used to escalate privileges within the system. Rootkits can be installed by malicious users, giving them future access to the system and the ability to hide their tracks. As a result, identifying files that have been altered by attackers and that may still be able to cause harm after an attack, are crucial components of security tools for HPC systems (Mildenberger, 2023). It should also be able to promptly identify instances of unauthorised user privilege escalation so that necessary action can be taken.

Mildenberger (2023), emphasises that it is never possible to ensure total security against all potential security flaws.

2.6 CURRENT LITERATURE IN SECURITY OF HPC SYSTEMS

To continue advancing performance, new technologies, such as emerging tools, sophisticated integration techniques, and computer architecture, are used in HPC systems (Yellu et al., 2019). Adopting new methodologies could make HPC systems more vulnerable to new security risks.

Many companies entrust their sensitive data and confidence to HPC systems. Trustworthy HPC hardware emerges as a vital technology challenge. HPC systems need a high computational capacity to perform better, (Yellu et al., 2019).
According to Yellu et al. (2019), unlike desktop computers, escalation attacks are the main threat to HPCs (especially multiuser HPC systems), which take advantage of flaws in the operating system by gaining the right of an administrator to potentially run or destroy the entire system.

The security needs of HPC systems vary from those of other communication systems as these computers are distinct systems, resources, and assets that could be targeted by an attacker (Yellu et al., 2019).

There are currently many software methods available to ensure HPC systems are secure. Unfortunately, software solutions may eventually be avoided in the future, or they may lead to new attack surfaces. Hybrid computing, which uses hardware accelerators and coprocessors to do large-scale parallel processing, is at the heart of HPC functionality. High performance is the focus of the designers and users of HPC systems (Yellu et al., 2019).

Malware can range from basic ads to rootkits that alter kernel control flow in a stealthy manner (Basu et al., 2020).
According to the authors, trusted hardware-based malware detection approaches have recently been developed on the

premise that bypassing software-based defences are easier than counterparts based on hardware.

The authors found that kernel rootkit malware can obtain complete control of a computer system by gaining unrestricted access to its resources, as a result, hardware-based malware detection solutions are gaining popularity. These methods presume that while an attacker may quickly modify software, manipulating hardware is more difficult.

Malware is used for a variety of reasons to disrupt computer systems regular behaviour, including amusement, notoriety, financial gain, and spying. The continuing development of new malware suggests that software-based solutions are not enough (Basu et al., 2020).

Researchers have begun to make use of capabilities included into reputable malware detecting devices. From an attacker's standpoint, when compared to software, it is harder to tamper with trusted hardware.
According to Sayadi et al (2018), malware detection at the hardware level has recently become a potential method for enhancing computing security. Increasing security without sacrificing performance is a challenge. (Vasilas et al. 2023).

Nolte et al. (2022), state that the main issue with handling sensitive data securely is that HPC systems are usually shared systems that are optimised for maximum performance rather than excellent security.

It is not secure to rely only on the conventional Unix permissions because new vulnerabilities are always being found, and over an extended period, new attacks are consistently uncovered that need new defences (Nolte et al., 2022).

Since administrators essentially have unlimited access, limiting system access does not fix the issue with data access. (Nolte et al., 2022). The authors believe that data integrity should be ensured even in the event of a privilege escalation that compromises a cluster.

2.7 CHAPTER SUMMARY

This chapter explored the literature on the topics of high performance computing, cloud computing, the literature of security in HPC and the cyber attacks. This research then explored what is the current literature in security of HPC systems. The research design and methodology of this research topic will be discussed in the next chapter.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 INTRODUCTION

The research approach is outlined in this chapter and the methods and techniques used in the systematic collection of data are described. The research methodology refers to the selection, in each research context, of values, assumptions, methods and techniques, and their use (Babbie & Mouton, 2001).

According to Neuman (2006, 2011), in the interpretive research paradigm, the most employed methodologies are qualitative and quantitative research approaches, with methodology selection influenced by the research problem, the type of data sources, the research question, the format source responses, and the necessary procedure analysis.

3.2 ONTOLOGY

According to Neuman (2011), ontology is the study of how to interpret the nature of reality. Two concepts that impact an ontological research perspective are objectivism and subjectivism. The author states that the essential question that informs ontology is whether existing social entities require subjective or objective perception.

According to Saunders et al. (2009), subjectivism is concerned with social phenomena that are formed by the perceptions and behaviours of those social actors who are interested in their existence, while objectivism, offers the notion that social entities exist independently and externally of the social dynamics that cause them to exist.

3.3 EPISTEMOLOGY

Epistemology is the study and understanding of what the universe is all about, and how truth emerges from its essence (Neuman, 2011). Its study is concerned with how humans acquire knowledge in the real world, and it entails everything that is required to generate knowledge about the truth (Bhattacherjee, 2012).

According to Wahyuni (2012), there are three epistemological views used in conducting research, namely, critical realism, interpretivism, and positivism.
This study follows a positivism approach to assist in gaining an in-depth understanding of the research context, including the collection of quantitative data.

3.4 PILOT STUDY

A pilot survey was conducted, and the intention was to provide the researcher with ideas of which questions to ask when conducting the final survey. The pilot survey offered a researcher with suggestions and insights that were not anticipated prior to the pilot study. These ideas and hints increase the probability of achieving clearer results in the research.

Due to the specific group targeted for this research, this pilot survey was conducted with five (5) HPC cluster administrators outside the number of those who participated in the official survey for this study. The questionnaire was used to acquire information on the participants understanding of the questions.
The overall results from the pilot survey were that questions are clear and understandable, with one suggestion of having an option of listed vulnerabilities as part of a checklist.

3.5 RESEARCH QUESTIONS

This research is based on the following research questions:

- What are the vulnerabilities in an HPC environment?
- How can these vulnerabilities affect HPC systems?
- Which types of threats these vulnerabilities attracted to HPC systems in the past?
- What could a potential solution to this problem look like?

3.6 RESEARCH DESIGN

According to Bhattacherjee (2012), there are two types of data collection techniques: positivist and interpretative. While the goal of interpretive methods such as action research and ethnography are to develop theories, positivist approaches like laboratory experimentation and survey research aim to evaluate hypotheses. Bhattacherjee (2012), states that positivist research techniques employ a logical approach to investigation, beginning with a theory and testing it using empirical data. In contrast, an inductive approach to interpretative approaches starts with the facts and works from the observable data to infer a theory about the phenomenon of interest.

These techniques are frequently mistakenly associated with both quantitative and qualitative research.
There are two categories of data that are acquired: quantitative and qualitative data, where quantitative data involve metrics and numeric scores, using structured interviews and observations as examples of data collection. Quantitative techniques like regression and qualitative techniques like coding are used to analyse the data (Bhattacherjee, 2012). According to the author, in positivist research, quantitative data is most used.
According to Neuman (2011), quantitative research is based on positivist ideas and emphasizes accurate measurement of variables and hypotheses. Creswell (2003) stated that Information can be measured and statistically analysed using quantitative research to either validate or invalidate claims. According to

Bhattacherjee (2012), the researcher should employ a variety of methods, including surveys, documents, secondary data, observations, and interviews, to gather both quantitative and qualitative data, regardless of the research design that is selected. The author further explains this by stating that the researcher may incorporate a few open-ended questions within a well-formed survey questionnaire intended to gather quantitative data. This will allow for the collection of qualitative data, which may yield unexpected insights that cannot be obtained from structured quantitative data alone.

Bhattacherjee (2012), states that operationalisation is the process of creating items or indicators to measure constructions. Indicators function at the empirical level, as opposed to ideas, which are conceptualised at the theoretical level. A variable is a set of indicators that indicate a specific construct at the empirical level. The values of attributes may be quantitative (numeric), and the variables are measured, and the relationship between them is quantified to test a theory (Hopkins, 2000).

Quantitative data analysis methods can be performed using methods like structural equation modelling and regression (Bhattacherjee, 2012).
Selecting the measurement level to be used is the first step in operationalising a construct. The values that an indicator can take are shown by these measurement levels (Bhattacherjee, 2012). For scientific measurements, Stanley Smith Stevens (1946) proposed four types of rating scales: nominal, ordinal, interval, and ratio scales.

Scale	Central Tendency	Statistics	Transformations
Nominal	Mode	Chi-square	One-to-one (equality)
Ordinal	Median	Percentile, non-parametric statistics	Monotonic increasing (order)
Interval	Arithmetic mean, range, standard deviation	Correlation, regression, analysis of variance	Positive linear (affine)
Ratio	Geometric mean, harmonic mean	Coefficient of variation	Positive similarities (multiplicative, logarithmic)
Note: All higher-order scales can use any of the statistics for lower order scales.			

Figure 3.1: Statistical properties of rating scales
Stanley Smith Stevens (1946)

For this study, the quantitative instrument used is informed by Stanley Smith Stevens (1946), proposed ordinal scales. This will assist the researcher in how to measure respondent's responses to predesigned items or indicators. Ordinal scales are used to measure data that is ranked (Bhattacherjee, 2012).

According to the author, it is impossible to analyse the real or relative values of characteristics, or the difference in attribute values. It is permissible to increase transformation in a monotonous manner, and percentiles and non-parametric statistics may be used in statistical analyses.

The author states that both validity and reliability—reliability being the degree to which a construct's measure is consistent or dependable—are necessary to provide adequate measurement of the constructs of interest. "Reliability implies consistency but not accuracy" (Bhattacherjee, 2012).

3.7 RESEARCH APPROACH

According to Saunders, Lewis, and Thornhill (2009), the inductive and deductive approaches are the two sorts of approaches that direct the research path to be taken. The inductive method focuses

on gathering empirical facts and developing a theory based on it. The deductive method is concerned with constructing a theory based on hypotheses and attempting to prove its validity (Creswell, 2009). The term "research approach" refers to the steps that are done from the broad thematic assumptions within research to the points of data collection, analysis, and interpretation.

3.7.1 Deductive

Within the positivist philosophical paradigm, a researcher may formulate a hypothesis to use deductive reasoning to support or refute a theory. This approach describes the phenomenon. As a research paradigm, positivism promotes the necessity for and resemblance of a common approach across all scientific fields, a form of thought that is especially prominent in the natural sciences (Saunders et al., 2009).

The researcher adopted a deductive approach for this study, and an investigation was conducted from 12 participants from different HPC cluster systems, to explore the type of attacks that tend to target them.

3.8 RESEARCH METHODS

The term "research methodology" describes an investigative procedure that starts with underlying assumptions and progresses to data collection and research design. A field of study that examines best practices for conducting research as well as the methods used by investigators to characterise, explain, and forecast events. (Myers, 2009).

According to Creswell (2003), knowledge claims, methods, and methodology all contribute to a research strategy that tends to be more a mixed approach, a quantitative, or qualitative approach.

3.8.1 Quantitative approach

In quantitative research, post-positivist assertions are largely used to create a study (i.e., the test of theories, cause and effect thinking, reduction to specific hypotheses, variables and questions, and the use of measurement and observation). As a result, the researcher applies investigative tactics such as experiments that produce statistical or numerical data (Creswell, 2003).
The author also states that hypothesis-testing research is a typical term for quantitative research. The study hypotheses are formulated based on theoretical claims, and an experimental design is subsequently built to evaluate the variables of interest while controlling for a subset of independent variables (Creswell, 2009). The principal instrument for data collection and analysis in quantitative studies is taken into consideration by the researcher (Creswell, 2003).

With this technique, the inquirer bases their claims on pragmatic grounds such as problem-oriented, pluralistic grounds, and consequence-oriented, and uses inquiry strategies that include collecting data either sequentially or simultaneously to best comprehend a study subject (Creswell, 2003). The distinction between qualitative, mixed, and quantitative approaches is based on the researcher's opinion, as each may contain a variety of methods, and neither is deemed intrinsically superior to the other. Based on the context, purpose, and type of the research study topic, the best approach is chosen (Hanson & Grimmer, 2007). The rationale for the research approach of this study will employ a quantitative research method of inquiry.

3.9 TRIANGULATION

Patton (1999) stated that triangulation is the process of using many approaches or data sources to develop a systematic understanding of events. Leedy and Ormrod (2005) supported this statement and went further to state that multiple sources of data are gathered in triangulation with the hope that they will all converge to support

diverse ideas, perspectives, or hypotheses. Triangulation was chosen as it would direct the observations, interpretation and allow this study to obtain greater reliability from the questionnaire sources to answer the research question.

3.10 DATA COLLECTION INSTRUMENTS

According to Welman and Kruger (2005), a questionnaire is a method for data collection with a set of questions designed to produce the data required to achieve the research goals. For this study, the questionnaire was used as the primary instrument for data collection, using an online questionnaire, based on Google Forms. The reason for this study to use a questionnaire was the advantage of generally permitting anonymity, due to the sensitivity of the topic.
A literature survey was used as a secondary instrument in collecting data from articles and journals.

3.10.1 Questionnaire Layout

The questionnaire was designed to measure the types of breaches that occur in an HPC system. The questionnaire structure and details can be found in Appendix A.

The questionnaire was subdivided into four (4) sections, with a total of 18 questions.
Section 1: consisted of one (1) question obtaining information about the demographics of the respondent.
Section 2: consisted of eight (8) multiple-choice questions to obtain information about security breaches.
Section 3: consisted of six (6) multiple-choice questions to obtain information about compromised systems.
Section 4: consisted of three (3) open-ended questions to obtain information from respondents about HPC environment vulnerabilities.

It was expected that participants would complete the questionnaire without assistance from the researcher, so all the questions were self-explanatory. Prior to sending out the official questionnaire, a sample questionnaire was evaluated with a small group of respondents who shared the same skills as the final questionnaire's intended audience. This was before putting the questionnaire online, to assist the researcher in determining if the questionnaire was fully understood.
The questionnaire was hosted on Google forms for a period of 3 weeks, from 26 September 2023 – 17 October 2023. There first week (26 September – 2 October) the questionnaire was sent out to be shared with the 16 participants, their other colleagues and contacts the researcher did not have. This week had the highest number of responders (8). The second week a reminder was sent out (3 October 2023), only 3 more responders. On the third week (17 October 2023 another reminder was sent out, receiving only 1 more responder, and by the end of that week the survey was closed with no further responses received.

3.11 SAMPLE DESIGN / UNIT OF ANALYSIS

Since the goal of the study is to investigate the type of security breaches that affect HPC cluster systems, it is crucial to choose people who have direct knowledge of or experience with the phenomenon being studied.
HPC cluster systems are the target population, and the sampling frame includes HPC cluster system users, security, and systems administrators in SADC country universities. Individuals who do not meet any of the following criteria are excluded from this study.

This study noted that, determining the precise population of high-performance computing (HPC) users, systems and security administrators in Africa is challenging, due to limited available data and the decentralised nature of HPC infrastructure across the continent.

With the limitations on precise population of high-performance computing (HPC) users, systems and security administrators in Africa, this study managed to identify a potential of 21 candidates. From the 21 potential candidates, 5 candidates were used for the pilot of the data instrument. This resulted in a total of 16 potential candidates who would participate on the questionnaire and only 12 participants responded to the survey.

3.12 DATA COLLECTION

In this study, the methods used in data analysis were based on the methods used for data collection. According to Panacek, (2008), a survey is a study consisting of asking people to respond to questions, this involves questionnaires and informal interviews written in writing, these can be formal or informal, internet-based, and anonymous. When conducting quantitative research, a researcher can collect data using three methods: questionnaires, observation, and interviews. The collection of data is a systematic method of collecting information that addresses pre-stated research questions, tests theories, and evaluates outcomes (Wilson, 2013). The data collection process should be conducted correctly using the right techniques to preserve scientific credibility, both primary and secondary sources of data were used in this research.

In this research, semi-structured questionnaires were used. Questionnaires can be used in any type of study, qualitative or quantitative, to collect data from many people while maintaining control over the responses. A questionnaire is a collection of comparable questions prepared to elicit information from respondents on a specific subject (Babbie, 2012).

The researcher sent out a total of 16 email requests prior to sending out the official questionnaire, asking for permission to participate in the data collection for this study. The 16 samples were a convenience sample, where the population of this study's

audience was those of HPC cluster systems administrators, security administrators and users whose email addresses the researcher had.

Following the initial request, the researcher then sent out an official email with a link to the questionnaire and a description of the survey's objective in the body of the message, Appendix A. The participants answered the online questionnaire, and the researcher was then able to corroborate and textually analyse the facts and figures using Google forms to export the answers to a spreadsheet and graphs to summarize the survey results.

3.13 DATA ANALYSIS

Ali (2020), descriptive statistics is the quantitative method of analysing a phenomenon that allows a researcher to methodically group, synthesise, and present observations. According to Moore, Notz and Notz (2006), important data findings are easier to grasp and communicate when presented visually, as in the case of summary tables and graphs, which are examples of descriptive statistics.

To be able to manage this, Pesamaa et al (2021), proposed four analysing steps that can be followed when data is analysed:

- Data collection
- Data preparation
- Data analysis
- Data discussion

Analysis of data refers to drawing conclusions from raw data (Wahyuni, 2012). As the data from the questionnaire was analysed, the questions on the questionnaire were categorised during the design of the questionnaire and so the data were grouped into different themes from those categories, discussed in the next chapter.

For data analysis, this study referred to the five phases that were proposed by, Pesamaa et al (2021): data preparation, data analysis, interpretation, and discussion.
Google Forms was used to create the survey. The participants were sent a link to the questionnaire through their email addresses that were obtained.

3.13.1 DELINEATION

The research only focused on security threats targeting HPC Systems deployed using OpenHPC in South Africa and SADC country universities. Sources of data are limited to HPC cluster systems administrators, security administrators, and users.

3.14 CHAPTER SUMMARY

The focus of methodology is on how research is done, how to find out about phenomena, and how to obtain information or how to collect data.
In this chapter, methodological approaches were explained, as well as the qualitative research was outlined. Questionnaires were used to gather data and all ethical considerations to conduct this questionnaire were followed. Methods of data analysis were also explained, and the data collected was analysed and will be given in the following chapter.

CHAPTER FOUR: RESULTS AND ANALYSIS

4.1 INTRODUCTION

This chapter documents and displays the information gathered through an online questionnaire. It will explain the findings and analyse the questionnaire, as well as the conclusions drawn from the examination of the responses of the 12 participants.
The statement of the research problem, research questions, and study purpose are listed below for the reader's convenience.

Statement of Research problem: There is a lack of classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.

Table 4.1: Research problem, research objective, and research questions

Research Problem	There is a lack of classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.

	Research Objective	**Research Questions**
	To contribute to guidelines towards the design of a security mechanism that can be used to prevent threats in HPC systems.	1. What are the vulnerabilities in an HPC environment? 2. How can these vulnerabilities affect HPC systems? 3. Which types of threats these vulnerabilities attracted to HPC systems in the past? 4. What could a potential solution to this problem look like?

4.2 Participants results

The questionnaire was sent to a total of 16 potential participants on different SADC universities using HPC cluster system.
All the participants were familiar with HPC systems, either as a user, systems, or security administrator of the system.

- Users: Users of HPC come from a broad range of industries, disciplines, and expertise levels. They all use HPC resources to further knowledge, solve complex problems, and drive innovation in their respective domains.
- Security administrators: Protecting HPC systems and data against security threats and vulnerabilities is the responsibility of security administrators, who are experts in this field.
- Systems administrators: Oversee designing, deploying, configuring, maintaining, and optimizing HPC infrastructure and resources are known as systems administrators.

Out of a target group of 16 (sent out request emails), 12 survey responses were received, Appendix B.

A systems administrator in this context is a person responsible for the upkeep, configuration, and reliable operation of the system. Security administrators monitor IT security and safety issues, ensuring that the information networks of their organisations remain secure from all sorts of cyber threats.

4.3 Findings

As stated in Chapter 3, the questionnaire question categories were developed and coded, and the findings were drawn, themes for discussion were identified.
Reporting findings is summarising and interpreting the results obtained from data analysis (Creswell & Creswell, 2021). Interpreting the survey findings in the context of the research objective, to identify patterns, trends, or relationships in the data and

draw conclusions based on the analysis, is used to refer, to a set of primarily quantitative methodologies: survey research (Creswell & Creswell, 2021).

In this section, the questionnaire responses collected during the research process are discussed. Based on the answers of the 12 participants, Appendix B, findings are drawn for each section of questions. The section is presented in such a way that the research objective (RO), research questions (RQs), and the questionnaire questions (Q.Qs) are linked as shown below.

Table 4.2: Research questions categorised into themes

RO: To contribute to guidelines towards the developme of a security mechanism that can be used to prevent threats in HPC systems.			
Research Questions	**Research questions**	**Questionnaire themes**	**Method**
RQ1	What are the vulnerabilities in an HPC environment?	Section 1: Demographics Section 2: Security breaches	Questionnaire
RQ2	How can these vulnerabilities affect HPC systems?	Section 3: Compromised system	Questionnaire
RQ3	Which types of threats these vulnerabilities attracted to HPC systems in the past?	Section 3: Compromised system	Questionnaire
RQ4	What could a potential solution to this problem look like?	Section 4: HPC environment vulnerabilities	Questionnaire

Table 4.3: Participants details

Participant	Occupation/ role
P1	Systems Administrator
P2	Systems Administrator
P3	Systems Administrator
P4	Systems Administrator
P5	Systems Administrator
P6	Security Administrator
P7	Security Administrator
P8	Management in HPC
P9	Scientist
P10	User in HPC
P11	Systems administrator
P12	Non HPC user

Briefly, skip logic was for participants to be kicked out if they do not work in an HPC environment. A total of 16 questionnaires were sent out and 12 came back, the 11 participants carried on with the questionnaire and only 1 participant was unable to continue as the survey ended at that point for them, Appendix A.

4.3.1 RQ1: What are the vulnerabilities in an HPC environment?

Q.Q1: What is your occupation/role?

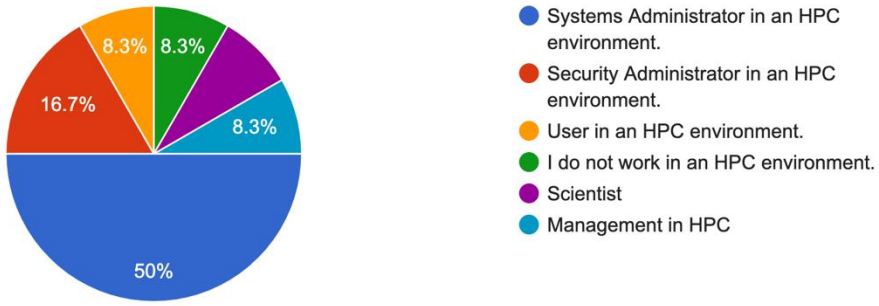

Figure 4.1: Occupation Comparison

The respondent's occupation or role is the key aspect of this demographic analysis since the information obtained regarding this question was able to help target the intended participants. The occupation has been reviewed and as indicated in *Figure 4.1*, the occupation of the respondents shows systems administrator respondents have dominated, with 50%, security administrator with 16.7%, management at 8.3% and Users in an HPC with 16.6% respondents.

Findings 1: About 91.6% of the respondents were either administrators or users for HPC systems.

Q.Q2: Indicate how many security breaches you have had in the last four years?

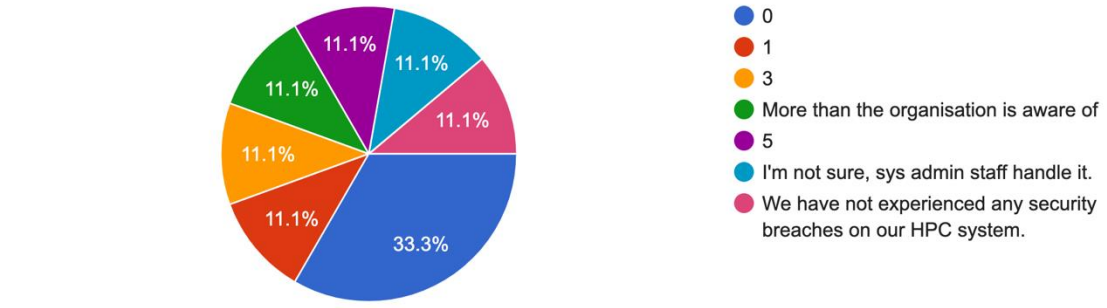

Figure 4.2: Security attacks or breaches in the last 4 years' comparison

To determine how many security breaches the target group had in the last four years. The question was asked using a scaled answer, Appendix A. The respondents had to answer according to their environment's security breaches.

According to *Figure 4.2,* 33.3% of the respondents have indicated that they have not had any security attack or breaches in their HPC environment in the last four years, while about 44.4% indicated that they have experienced a security breach on their system. Although millions of security attacks target these types of systems every day, they do not always manage to penetrate or compromise the system. The above results are for those attacks that have managed to penetrate the system even though some form of security protection was used.

The data collected, shows that there were more than two security attacks or breaches that were listed by the respondents in the last four years.

Findings 2: Almost half of the respondents indicated a security breach in their HPC system during the last four years.

Q.Q3: Complete this question only if you had **one** of the following security attacks or breaches in the last four years. Please select which breach you have seen on your system.

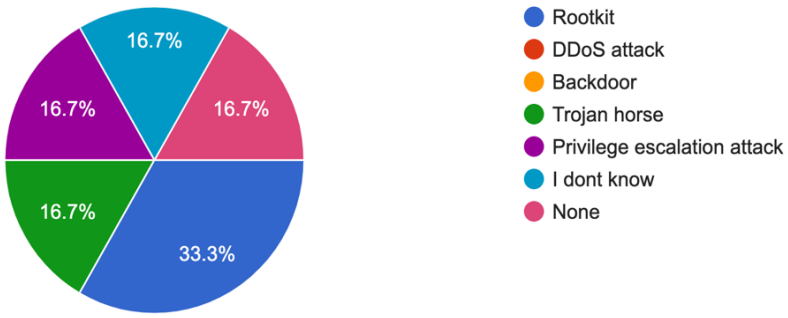

Figure 4.3: One security attack or breach in the last 4 years' comparison

From this question, the researcher wanted to determine which type of security attack or breach that is listed by the respondents from those that manage to penetrate the system, in the last four years. The question was asked using a multiple-choice answer that listed known attacks Appendix A. *Figure 4.3* shows that only 6 respondents answered this question. About 66.7% of the respondents represented by 4 survey participants, who indicated that they have had *one* security breach in their system. The selected security attack or breach was from two rootkit attacks, one privilege escalation attack and one trojan horse attack. One participant was not sure while the other indicated no attack in the last 4 years.

Findings 3: The Rootkit, Trojan horse and Privilege escalation attacks are the main common breaches from those who experienced one attack.

Q.Q4: Complete this question only if you had a **second** of the following security attacks or breaches in the last four years. Please select which breach you have seen on your system.

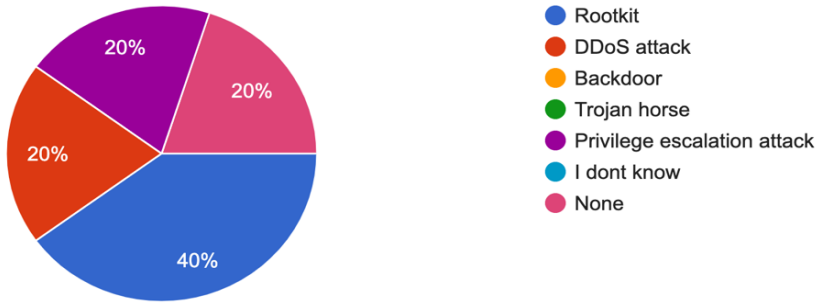

Figure 4.4: Second security attack or breach in the last 4 years' comparison

From this question, the researcher wanted to determine which type of second security attack or breach, that is listed by the respondents from those that manage to penetrate the system, in the last four years. The question was asked using a multiple-choice answer that listed known attacks, Appendix A. *Figure 4.4* shows that only 5 respondents from the 12 answered this question. About 40% of the respondents represented by 2 survey participants and for each 20% representing a single (1) participant, who indicated that they had a *second* security breach in their system. The selected security attacks or breaches were from rootkit attacks, one privilege escalation attack and one DDoS attack, with one participant indicating no second attack in the last 4 years.

Findings 4: Privilege escalation, Rootkit and DDoS attacks are the common security breaches from those who experienced a second attack.

Q.Q5: Complete this question only if you had a **third** one of the following security attacks or breaches in the last four years? Please select which breach you have seen on your system.

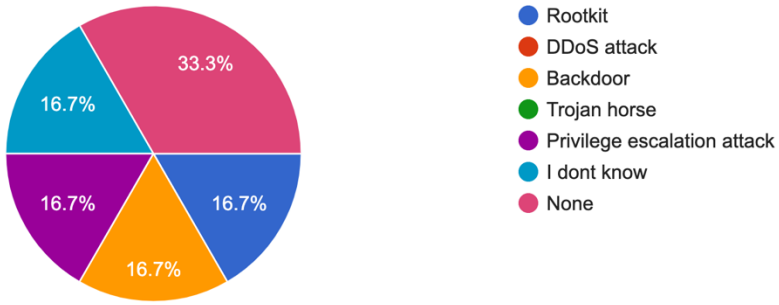

Figure 4.5: Results of the third security attack or breach in the last 4 years

From this question, the researcher wanted to determine which type of third security attack or breach, that is listed by the respondents from those that manage to penetrate the system, in the last four years. The question was asked using a multiple-choice answer that listed known attacks, Appendix A. *Figure 4.5* shows that only 6 respondents from the 12, answered this question. About 33.3% of the respondents represented by 2 participants indicated no third attack in the last 4 years. One (1) participated did not know the answerer, while the remaining 3 participant each listed the rootkit attack (16.7%), backdoor breach (16.7%) and privilege escalation attack (16.7%).

Findings 5: Privilege escalation, Rootkit and Backdoor attacks are the common security breaches from those who experienced a third attack or breach.

Q.Q6: How was the first attack detected?

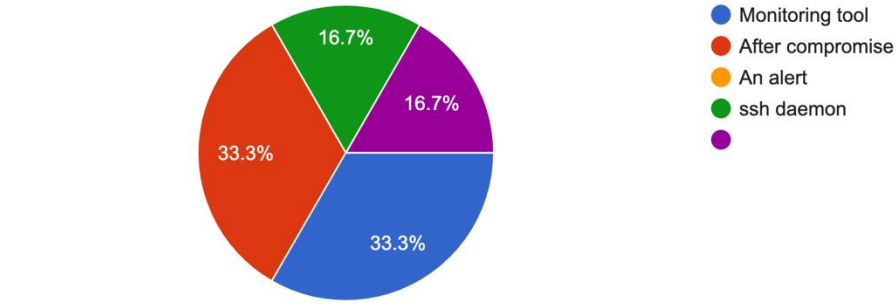

Figure 4.6: Detection of first attack or breach comparison

The researcher wanted to determine the type of tools used to detect or pick up the first security attack or breach. The question was asked using a multiple-choice answer that listed known tool types, Appendix A. The comparison in the pie chart with a total of 6 responses, *Figure:* two (2) participants represented by the 33.3% of responders indicated that the *one* breach was identified from a monitoring tool, and 2 participants represented by 33.3% indicated that the attack was detected after the compromise. Another participant represented by 16.7% indicated another monitoring options outside the ones that were listed, the “ssh daemon”, while the last participant represented by 16.7% gave no answer to the question.

Findings 6: The monitoring tool and ssh daemon did help on picking up the security breach and others were only discovered after the compromise.

Q.Q7: How was the second attack detected?

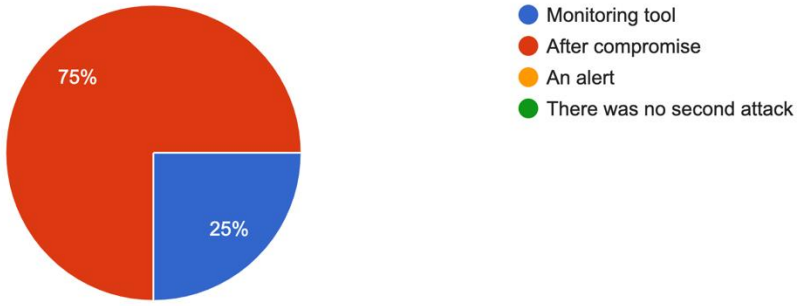

Figure 4.7: Detection of the second attack or breach comparison

The researcher wanted to determine the type of tools used to detect or pick up the *second* security attack or breach. The question was asked using a multiple-choice answer that listed known tool types, Appendix A. With only 4 participants responding to this question, the comparison in *Figure 47,* indicates that the *second* system attack or breach was picked up after the system was compromised, represented by 75% (3 participants), and the 25% (1 participant) detected the second breach from monitoring tool.

Findings 7: Second attacks managed to compromise the system, while one system was helped a monitoring tool to detect the security breach.

Q.Q8: How was the third attack detected?

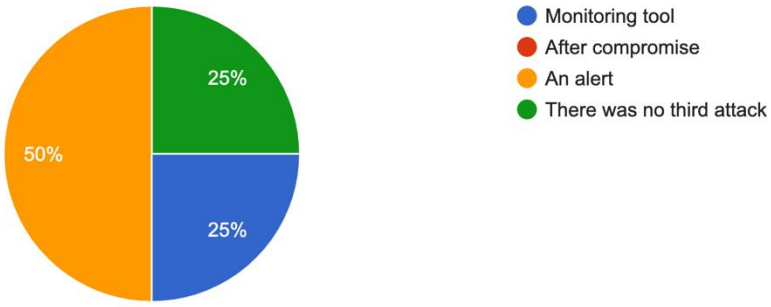

Figure 4.8: Detection of the third attack or breach comparison

The researcher wanted to determine the type of tools used to detect or pick up the third security attack or breach. The question was asked using a multiple-choice answer that listed known tool types, Appendix A. With only 4 participants responding to this question, the comparison in Figure 4.8, indicates that the third system attack or breach was detected, and an alert received, represented by 50% (2 participants), and 25% (1 participant) indicated the third breach was seen in the monitoring tool used.

Findings 8: Third attacks were detected by the monitoring tool and the alerting system before it managed to compromise the system.

Q.Q9: In the last four years, what have been the tools used to identify or protect against a potential insider attack targeting the system?

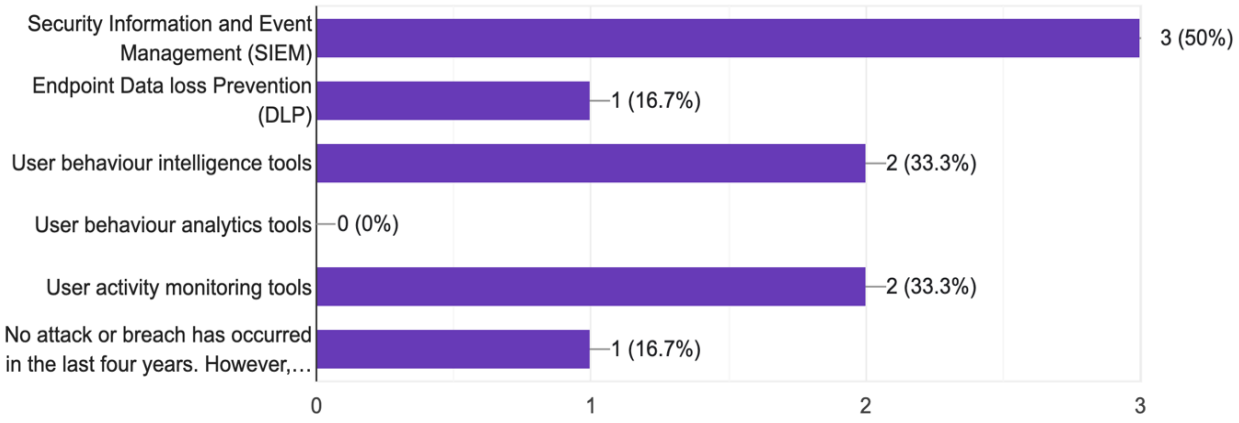

Figure 4.9: Comparison of security tools used for insider attacks

Figure 4.9, respondents who answered this question show that the Security Information and Event Management (SIEM) was the most used tool at 50% to help protect against insider attacks that are intentional or unintentional.

This tool provides real-time analysis of security alerts produced by network hardware and applications. The other tools used at both 33.3%, was the User Activity Monitoring (UAM) and User Behaviour intelligence (UBE) which are software tools that monitor and records the actions of end-users on computers, networks, and other company-owned IT resources. These tools are mostly implemented to help detect and avoid insider security threats, whether they are unintentional or with malicious intent. One user at 16.7% indicated that although no attacks have occurred in the last four years, they

have proceeded to strengthen their HPC system's security with preventative measures.

Findings 9: Security Information and Event Management is the most used tool for an insider attack, followed by the user activity monitoring and user behaviour intelligence tool. Then the endpoint data loss prevention (DLP) was indicated by one participant that it's a tool they still use, while the user behaviour analytics tool was at 0%.

4.3.2 RQ2: How can these vulnerabilities affect HPC systems?
4.3.3 RQ3: Which types of threats these vulnerabilities attracted to HPC systems in the past?

Q.Q10: What damage has been caused by the first attack which has managed to compromise the system?

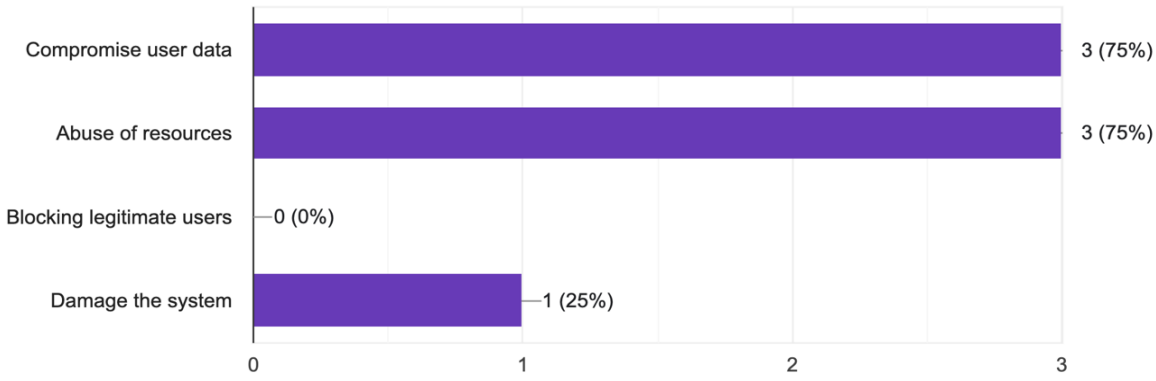

Figure 4.10: Comparing the damage caused by the first security attack or breach

The researcher wanted to determine what kind of impact was caused by the *first* security attack that managed to compromise the system. The question was a multi-choice consisting of a list of options, Appendix A. According to *Figure 4.10*, most of the participants who answered, listed both the abuse of resources, and compromised user data as the top intention of the perpetrators. The damaging of the system was also listed as one of the main purposes of the first attack that penetrated the system.

Findings 10: The rootkit, privilege escalation and trojan horse attack managed to block legitimate users and abuse HPC resources.

Q.Q11: What damage has been caused by the second attack which has managed to compromise the system?

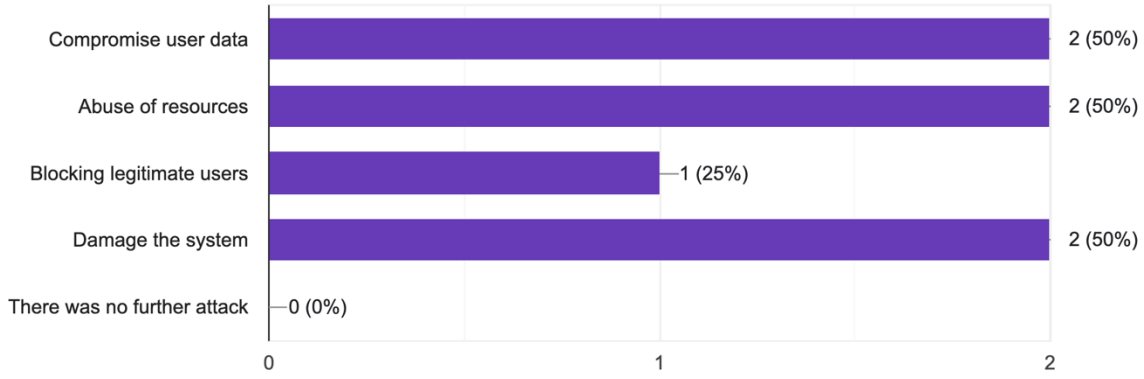

Figure 4.11: Comparing the damage caused by the second security attack or breach

The researcher wanted to determine what kind of impact did the *second* security attack that managed to compromise the system. This question was a multi choice consisting of a list for respondents to choose from, Appendix A. According to *Figure 4.11*, respondents

who specified that they did experience a second security breach in the last four years, answered that the abuse of resources, compromise of user data and damage to the system were the main intention of the intruders. One system experience access issue for legitimate users.

Findings 11: Rootkit, Privilege escalation and DDoS attacks managed to compromise the system and cause disruption.

Q.Q12: What damage has been caused by the third attack which has managed to compromise the system?

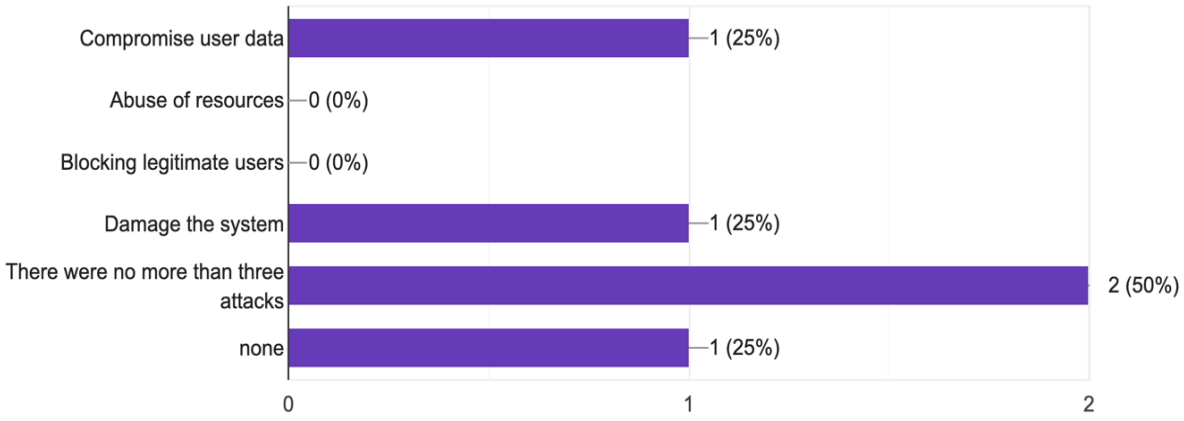

Figure 4.12: Comparing the damage caused by the third security attack or breach

The researcher wanted to determine what kind of impact did the *third* security attack cause that managed to compromise the system. This question was a multi choice consisting of a list for respondents to choose from, Appendix A. According to *Figure 4.21*, respondents who specified that they did experience a third security breach in the last four years, answered that the abuse of resources, compromise

of user data and damage to the system were the main intention of the intruders.

Findings 12: Rootkit, Privilege escalation and backdoor attacks managed to compromise the system and caused disruption.

Q.Q13: How long has the first attack kept the system offline?

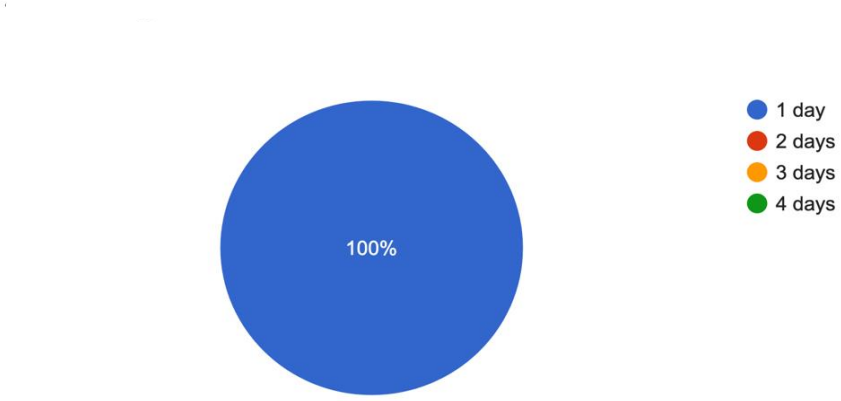

Figure 4.13: Duration of the system offline from the first attack or breach

The purpose of this question was for the researcher to understand how long the first security breach or attack when it had compromised the system, can take to be mitigated, Appendix A.

Findings 13: The system interruption and loss of user data cost the system unplanned downtime of one day by system breaches.

Q.Q14: How long has the second attack kept the system offline?

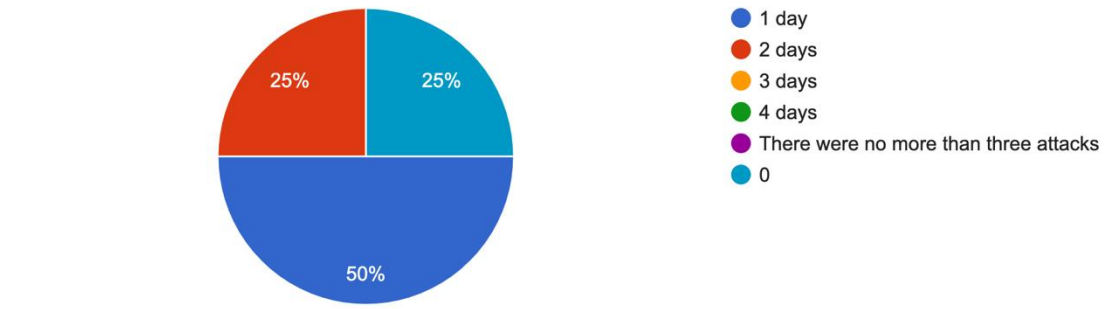

Figure 4.14: Duration of the system offline from the second attack or breach

The purpose of this question was for the researcher to understand how long the second security breach or attack when it had compromised the system, can take to be bring the system back online, Appendix A.

Findings 14: The system interruption and loss of user data cost the system unplanned downtime of between one to two days from these system breaches.

Q.Q15: How long has the third attack kept the system offline?

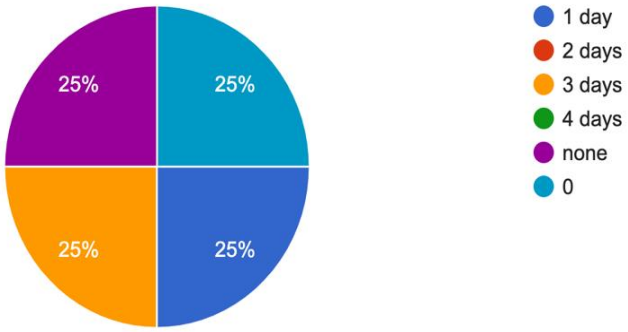

Figure 4.15: Duration of the system offline from the third attack or breach

Findings 15: The system interruption and loss of user data cost the system non-operational hours of between one to three days from these system breaches.

4.3.4 RQ4: What could a potential solution to this problem look like?

Q.Q16: What are some of the challenges you encounter in protecting such a system in this environment?

According to participant (P) P6 and P7, it is a challenge to efficiently protect and monitor a diversity of users who have different but valid patterns of use. They find that these systems are complex with continuous evolving threat that bring new hacking methodologies that cannot be detected by traditional security controls. P6, P7 and P8 also find user access control being an issue, with P6 stating that “users with legitimate access misuse their privilege”. P1 and P10 believe the issue lies in the lack of security skills required to know what to do. While P2 states that it’s

the “Inadequacy of tools addressing data loss (Data integrity)” and data privacy compliance (P7). P6 and P7 state that mitigating insider threats is a significant concern. P7 goes on and finds that challenges are coming from inadequate patch management processes, tools impacting on system performance. P9 stated that as a user they do not know but wouldn’t want experience data loss. Users are considered a very big vulnerability with these systems, where they can be careless at times with their system credentials, sharing of created accounts, or leaving unencrypted passwords.

Findings 16: System users are the main security challenge for administrators.
Findings 17: HPC security is more complex than what traditional security controls can handle.

Q.Q17: In your opinion, what are the vulnerabilities currently in HPC systems?
According to P6, users are the main vulnerability, “using weak passwords, sharing credentials, or inadvertently exposing sensitive data”. P1 found that using open-source tools to monitor the system, opens gap to system vulnerabilities. P6 and P7 states that current vulnerabilities are on complex system architecture that, if not properly configured or patched, can expose system to malicious activity, especially with the ever-evolving cyber threats. Weak system access policies, can lead to the success of brute force attack, according to P2 and service like SSH, says P6.
P6 finds that HPC system “schedulers used to manage and distribute computing tasks across system nodes can be targeted for privilege escalation and unauthorised access”.

HPC systems run a lot of legacy applications, which can be a loophole for security vulnerabilities that cannot be removed since these software’s are still valid for research. P6 also support this statement mentioning vulnerabilities that could be found in firmware or software stack.

Findings 18: Misconfigurations caused by human error.
Findings 19: The hardware has security vulnerabilities that are prone to attacks.
Findings 20: Users still run legacy software in HPC systems.

Q.Q18: In your opinion, what could be the best solution/s to address these vulnerabilities?
Regular security awareness and trainings for both systems users and administrators. This will help in enhancing their awareness and mitigating the risk, this is according to P6, P7 and P9. P3 believe that HPC users need more stringent login procedures, such as the use of multi-factor authentication (MFA)

P3, P6, P7 and P8 state that the implementation of robust access control measures and user activity monitoring tools, can help in addressing some of the vulnerabilities that these systems have. It is important to always stay up to date with evolving cybersecurity threats, says P2 and P7. It is important to to invest in security and much as the performance. Performing of regular system and security updates, can help in rectifying any misconfigurations before they get exploited, says P6.

P2, P6 and P7 also recommend regular updates and patch management for these systems like updating kernel, OS, and hardware firmware to counter bugs and other vulnerabilities. While P7 goes further and recommends developing comprehensive strategy to mitigate system insider threats and attacks.

Findings 21: User behaviour and activity monitoring.
Findings 22: Security awareness and trainings.

4.3.5 Summary of findings

RQ1: What are the vulnerabilities in an HPC environment?

Note: the first Q below refers to the questionnaire question number.

Q.Q1: What is your occupation/role?

Q.Q2: Indicate how many security breaches you have had in the last four years?

Q.Q3: Complete this question only if you had **one** of the following security attacks or breaches in the last four years. Please select which breach you have seen on your system.

Q.Q4: Complete this question only if you had a **second** of the following security attacks or breaches in the last four years. Please select which breach you have seen on your system.

Q.Q5: Complete this question only if you had a **third** one of the following security attacks or breaches in the last four years? Please select which breach you have seen on your system.

Q.Q6: How was the first attack detected?

Q.Q7: How was the second attack detected?

Q.Q9: In the last four years, what have been the tools used to identify or protect against a potential insider attack targeting the system?

Table 4.4: Findings of RQ1

Findings no.	Findings
Finding 1	About 91.6% of the respondents were either administrators or users of HPC systems.
Finding 2	Almost half of the respondents indicated a security breach in their HPC system during the last four years.
Finding 3	The Rootkit, Trojan horse and Privilege escalation attacks are the main common breaches from those who experienced one attack.
Finding 4	Privilege escalation, Rootkit and DDoS attacks are the common security breaches from those who experienced a second attack.
Finding 5	Privilege escalation, Rootkit and Backdoor attacks are the common security breaches from those who experienced a third attack/ breach.
Finding 6	The monitoring tool and ssh daemon did help on picking up the security breach and others were only discovered after the compromise.
Finding 7	Second attacks managed to compromise the system, while one system was helped by a monitoring tool to detect the security breach.
Finding 8	Third attacks were detected by the monitoring tool and the alerting system before it managed to compromise the system.
Finding 9	Security Information and Event Management is the most used tool for an insider attack, followed by the user activity monitoring and user behaviour intelligence tool. Then the endpoint data loss prevention (DLP) was indicated by one participant that it's a tool they still use, while the user behaviour analytics tool was at 0%.

RQ2: How can these vulnerabilities affect HPC systems?

RQ3: Which types of threats these vulnerabilities attracted to HPC systems in the past?

Q.Q10: What damage has been caused by the first attack which has managed to compromise the system?

Q.Q11: What damage has been caused by the second attack which has managed to compromise the system?

Q.Q12: What damage has been caused by the third attack which has managed to compromise the system?

Q.Q13: How long has the first attack kept the system offline?

Q.Q14: How long has the second attack kept the system offline?

Q.Q15: How long has the third attack kept the system offline?

Table 4.5: Findings of RQ2 and RQ3

Findings no.	Findings
Finding 10	The rootkit, privilege escalation and trojan horse attack managed to block legitimate users and abuse HPC resources.
Finding 11	Rootkit, Privilege escalation and DDoS attacks managed to compromise the system and cause disruption.
Finding 12	Rootkit, Privilege escalation and backdoor attacks managed to compromise the system and caused disruption.
Finding 13	The system interruption and loss of user data cost the system unplanned downtime of one day by system breaches.
Finding 14	The system interruption and loss of user data cost the system unplanned downtime of between one to two days from these system breaches.
Finding 15	The system interruption and loss of user data cost the system non-operational hours of between one to three days from these system breaches.

RQ4: What could a potential solution to this problem look like?

Q.Q16: What are some of the challenges you encounter in protecting such a system in this environment?

Q.Q17: In your opinion, what are the vulnerabilities currently in HPC systems?

Q.Q18: In your opinion, what could be the best solution/s to address these vulnerabilities?

Table 4.6: Findings of RQ4

Findings no.	Findings
Finding 16	Results shows users as the main security challenge for administrators.
Finding 17	Results shows that HPC security is more complex than what traditional security controls can handle.
Finding 18	Results shows misconfigurations mainly resulted from human error.
Finding 19	Results shows that the hardware has security vulnerabilities that are prone to attacks.
Finding 20	Results shows that users still run legacy software in HPC systems.
Finding 21	Resulted to user behaviour and activity monitoring.
Finding 22	Resulted to security awareness and trainings

4.3.6 Summary of findings theme developed

In this chapter, the information used for the research is discussed. Data from the questionnaire (consisting of 18 questions and answered by 12 participants) conducted during the research process were analysed. Twenty-two (22) findings are identified based on the analysis of the data. Four (4) themes are developed from the (22) findings. These four themes are as follows:

Table 4.7: Findings categorised into themes.

RO: To contribute to guidelines towards the design of a security mechanism that can be used to prevent threats in HPC systems.			
Research Questions	**Research questions**	**Questionnaire themes**	**Finding themes**
RQ1	What are the vulnerabilities in an HPC environment?	Section 1: Demographics Section 2: Security breaches	Complex architecture and Users
RQ2	How can these vulnerabilities affect HPC systems?	Section 3: Compromised system	Resource abuse and data loss
RQ3	Which types of threats these vulnerabilities attracted to HPC systems in the past?	Section 3: Compromised system	Rootkit, Privilege escalation, Backdoor attack, and DDoS attacks
RQ4	What could a potential solution to this problem look like?	Section 4: HPC environment vulnerabilities	HPC security methodologies

Table 4.7 shows the relationship between the research objective, research questions, questionnaire themes and findings theme. The finding themes, *Complex architecture and Users,* Resource abuse and data loss*, Rootkit, Privilege escalation, Backdoor attack, and DDoS attacks* and the *HPC security methodologies*, guides the answer to the RO of this study.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

From the findings described in Chapter 4, four themes have been identified. The themes are:

5.1.1 Complex architecture and Users

5.1.2 Resource abuse and data loss

5.1.3 Rootkit, Privilege escalation, Backdoor attack, and DDoS attacks

5.1.4 HPC security methodologies

In Chapter 5, the above themes are discussed and then linked to the research questions and then main objective of this study. For the convenience of reading the research problem, research questions, and the research objective of the study are listed below:

Research problem: There is a lack of classification of hardware security breaches, which leads to uncertainty of where to focus efforts to protect against HPC system attacks.

RO: To contribute to guidelines towards the design of a security mechanism that can be used to prevent threats in HPC systems.

RQ1: What are the vulnerabilities in an HPC environment?
RQ2: How can these vulnerabilities affect HPC systems?
RQ3: Which types of threats these vulnerabilities attracted to HPC systems in the past?
RQ4: What could a potential solution to this problem look like?

5.2 The Themes

5.2.1 Theme 1: Complex architecture and Users

RQ1: What are the vulnerabilities in an HPC environment?

Users are one of the biggest vulnerabilities to these systems. While you can get other users who are concerned about how secure the

system is, may still prioritise getting their tasks processed by these machines and getting to the results. This research finds that users are entrusting most aspects of system security to be handled by the administrators of the system. Regarding the security challenges they encounter as a user. P9 said “As a user I don't know but we wouldn't like an attack that deleted our data either through targeting our users or just indiscriminate deletion.” (Appendix B).

Entities offering High Performance Computing (HPC) services need to invest in the culture of regular security awareness training for their users. P7 supports this statement, saying “Educate users to enhance their awareness of security best practices” (Appendix B).

According to Hwang et al (2021), the goal of information security awareness is to empower individuals to identify potential security flaws or issues and take the necessary action in response. Due to the continuous evolving of these threats to the system, it is important for the users to collaborate with the system/ security administrator to mitigate the challenges of protecting the system.
One aspect that most participants do agree on is that security awareness training needs to be introduce for HPC users.

Archiving the ability for a system to provide high performance computing, requires combination of different hardware components and applications performing in a smallest time possible, it introduces complexity. This study found that the working environment differs greatly from a typical IT setting. P7 said “Challenges in safeguarding our HPC system include complexity, evolving threats..” (Appendix B).

According to Nolte et al. (2022), The main issue with handling sensitive data securely is that HPC systems are usually shared systems that are optimised for maximum performance rather than excellent security. Depending on the missions these systems support, their designs may vary, and security solutions customised, to meet the needs of the HPC system.

P7 also mentions that some of the challenges include “resource constraints, performance impact…” (Appendix B). The resources are shared by various system users and because of the performance optimisation, it is frequently the case that users communicate directly with the host's operating system (Nolte et al. 2022). The author states that these system users are somewhat trustworthy, any local weakness can be quickly taken advantage of by users or bots who have obtained access to user credentials.

It seems that there is a lack of user awareness when it comes to their responsibilities in security. Ponce and van Zon (2023), state that many times, end users of remote computing systems are unaware of simple solutions to improve security against cyberattacks and threats. The need for educating users has been expressed. The authors believe that the complexity and quantity of cyberthreats are both increasing at a rapid rate. Finding vulnerabilities is essential to comprehending attacks and defences against them.

Li et al. (2015:7) states that there are several hardware threats that must be fought against to preserve the system's maximum efficiency, hardware security is an essential component of a properly secured HPC environment. The user and their actions are the most susceptible component in this situation and systems that have vulnerabilities are weak points or flaws. Users won't know best practices or how to use these systems cautiously without training (Ponce and van Zon, 2023).

5.2.2 Theme 2: **Resource abuse and data loss**

RQ2: How can these vulnerabilities affect HPC systems?

A vulnerable system can be a target for attacks that can exploit those weaknesses to misuse resources or steal data. According to Ponce and van Zon (2023), vulnerabilities may result from poor designs, neglected system components, bugs, or unanticipated use cases. P6 said “2,Service like SSH, running on HPC systems may have

vulnerabilities if not properly configured or patched. 3. Vulnerabilities in job schedulers used to manage and distribute computing tasks across nodes can be targeted for privilege escalation and unauthorized access. 4. Incorrectly configured systems" (Appendix B). It is important to keep up to date with patches and updates for HPC systems, as the goal of security is always changing due to continuous growth of cyberattacks.

The authors state that there are many types of cyberattacks that can be classified in two basic categories: one in which the intention of the attack is to affect availability (e.g. through stopping a specific system functionality), or an attack with the intention of compromising integrity or confidentiality (e.g. gaining unauthorised access to system or user data). P7 and P8 believe that the current vulnerabilities are in the access control management and data storage safety.

Literature shows that the risks associated with gaining access to a service depend on the level of authorisation held by the person whose credentials were compromised. Normal system users would only have access to their own data or data that is shared with them, and the breach impact could be limited to their account, while system administrators may have elevated access, it would be far riskier to hack their accounts, and affect multiple users or the entire system.

According to Ponce and van Zon (2023), unintentional security flaws in the operating system or software used in the service could allow common users to escalate their privileges to administrator level. Among the distinctive goals of cybersecurity attacks are resource abuse and user data access.

It is important for system and security administrators to comprehend the mission these systems support, the applications they run, and their design. This will help in identifying the vulnerabilities associated with their HPC environment. Ponce and van Zon (2023), advise that weighing the cost of preventative measures and the impact on

usability against the risks and severity of a breach is necessary.

5.2.3 Theme 3: Rootkit, Privilege escalation, Backdoor attack, and DDoS attacks

RQ3: Which types of threats these vulnerabilities attracted to HPC systems in the past?

Mildenberger (2023:3) stated that users of HPC systems are geographically dispersed and connect to the system via the public internet. Insiders with authorised access to the system and outsiders with unauthorised access can be used to identify malicious users. The types of attacks that were found in this study are still some of the main HPC security problems mentioned in current literature.

It seems the reasons why attackers have mostly adapted DDoS attack on such systems, they are more complex variant that involves launching DoS attacks from multiple, dispersed servers because repeated traffic from a single IP could easily raise flags and be stopped. Literature sates that some of the applications used in HPC systems are legacy software that can have vulnerable source codes. According to Ponce and van Zon (2023), malware may enter a computer through unintentional installation, such as through components of other software packages.

It is important for systems and security administrators to understand the current trends and mitigations for HPC systems. P2 support this by stating that “staying up to date/ alert with HPC vulnerables and create patches to avoid the exploitation of that said vulnerability” (Appendix B). According to Ponce and van Zon (2023), cyberattacks can be difficult to identify and, once they cause harm, difficult to repair. There is no way to ensure that a system is 100% impervious to attacks, and implementing extremely strict measures may compromise its usability.

The authors advise that trying to reduce the likelihood of such attacks succeeding is the best course of action.

5.2.4 Theme 4: HPC security methodologies

RQ4: What could a potential solution to this problem look like?

In an endeavour to answer RQ4, Mildenberger (2023:14), recommends an essential component of an HPC systems security is a scalable intrusion detection system (IDS) solution. This study is noting that IDS is only one component of an integrated security solution, and other components are needed as well.

It should be mandatory to do OS or software updates. P7 states that: “Ensure timely updates and patch management for system components” (Appendix B). Attackers frequently use outdated operating systems and security patches to their advantage, taking advantage of security flaws that could have been fixed with a straightforward OS or application update (Ponce and van Zon, 2023).

The literature recommends an additional layer of authentication when accessing the system is the Multi Factor Authentication (MFA). It permits the use of biometric elements for user authentication, including fingerprint sensors, iris scanning, and facial recognition. P3 and P4 have recommended using authentication management tools such as the MFA.

Ponce and van Zone (2023), recommend having processes like configuration management in place and tools like rootkit scanning, root access restrictions, and other techniques to reduce the risk of malware attacks. P7 advises on mitigations by developing comprehensive strategies. The authors believe it is imperative to acknowledge that a system is just as strong as its weakest component when utilising shared resources and gaining remote access to them. For this reason, considering the application of the combined tactics and strategies.

5.2.5 RO: To contribute to guidelines towards the design of a security mechanism that can be used to prevent threats in HPC systems

The security vulnerability between these systems and users needs to be addressed. Although the HPC institutions have policies in place for using them, some part of the responsibility to archive protection against cyber attacks lies with them, as a system is just as strong as its weakest component.

The following recommendation are guidelines towards a security mechanism of defence from the findings of this study:

5.2.5.1 Secure authentication: ensuring the identification of an entity, an administrator, a user, process, a program, server, etc

5.2.5.2 Awareness and Responsibility: Users should be aware of the impactful role they play in securing these systems

5.2.5.3 Integrity check technique: ensuring transmitted data is reliable and unaltered

5.2.5.4 HPC system security audit: rectifying any misconfigurations and identifying vulnerabilities

By adopting the guidelines mentioned above, a security mechanism of defence for HPC system can institute a culture of security for their environment.

5.3 Reflection of this study

It is important to realise that cybersecurity is continuously evolving and investing in the culture of security in HPC environment is a long-term process that needs to be ongoing.

This study found that HPC systems and environments often have distinct security needs based on their mission and they adhere to their systems separate security guidelines. This has opened a door to a question such as “How can the HPC community address the gap in the exchange of information and security solutions?”. Further research on the same topic at HPC systems in the top 500 list of the fastest super computers in the world can be conducted as well.

5.4 Limitation of research

It is important to recognise a few study limitations. Because the 12-sample size is rather small, and one should exercise caution against generalisation when interpreting the results. This study had been conducted on the HPC cluster systems in the Ecosystem project of SADC country universities and had no access to direct email contacts of systems and security administrators or users using the systems currently listed on the top 500 Supercomputers list.

5.5 Conclusion

In this study, there are guidelines that were identified contributing towards a framework development that classifies hardware security breaches in HPC systems. Further research question was also identified. These guidelines towards a framework development that classifies hardware security breaches in HPC systems can be further added with more research on this topic. The study has provided a summary of the most common cyber threat categories affecting HPC systems. We covered several useful approaches that users and administrators can employ to lessen the impact of some of these attacks getting on the HPC systems.

Although some approaches are commonly known and extensive research have been done on them, several HPC users has backgrounds in a variety of fields and require training in applying them. The study believes by placing system users in the perspective of the risks and effects, they will become more aware of them, which will ultimately benefit the entire HPC environment and community of system users. It is strongly advised to follow the guidelines provided here towards strengthening security design mechanisms for HPC systems and its user's overall cybersecurity posture.

6. BIBLIOGRAPHY/REFERENCES

Aljumah, A. and Ahanger, T.A., 2020. Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*, *14*(7), pp.1185-1191.

Ali, A., 2020. Quantitative Data Analysis. *University of Sindh*, pp.1-10

Alves, T. & Morris, T. 2018. Hardware-based Cyber Threats. In *ICISSP.* 259-266.

Ansari, M.T.J., Pandey, D. & Alenezi, M., 2018. STORE: Security Threat Oriented Requirements Engineering Methodology. *Journal of King Saud University-Computer and Information Sciences.*

Al-Jody, T., Holmes, V., Antoniades, A. and Kazkouzeh, Y., 2020, December. Bearicade: secure access gateway to High Performance Computing systems. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1420-1427). IEEE.

Aljumah, A. and Ahanger, T.A., 2020. Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*, *14*(7), pp.1185-1191.

Basu, K., Krishnamurthy, P., Khorrami, F. & Karri, R., 2020. A theoretical study of hardware performance counters-based malware detection. *IEEE Transactions on Information Forensics and Security*, *15*, pp.512-525

Babbie, E. and Mouton, J., 2001. The practice of social research: South African edition. *Cape Town: Oxford University Press Southern Africa*.

Bhattacherjee, A., 2012. *Social science research: Principles, methods, and practices.*

Bennett, E.E. and McWhorter, R.R., 2016. Opening the black box and searching for smoking guns: Process causality in qualitative research. *European Journal of Training and Development*, *40*(8/9), pp.691-718.

Burt, J. 2017. *An Adaptive Approach to Bursting HPC to the Cloud. The Next Platform.* https://www.nextplatform.com/2018/02/26/adaptive-approach-bursting-hpc-cloud/ [26 February 2018].

Bulusu, R. Jain, P. Pawar, P. Afzal, M. & Wandhekar, S. 2018. *Addressing Security Aspects for HPC infrastructure.* 2018 International Conference on Information and Computer Technology. 27-30.

Buyya, R., 1999. High performance cluster computing. *New Jersey: F'rentice*.

Bradford, A. 2017. Live Science Contributor. https://www.livescience.com/21569-deduction-vs-induction.html [23 January 2020].

Creswell, J.W., 2009. Mapping the field of mixed methods research.

Dong, F. Zhou, P. Liu, Z. Xu, Z. & Lou, J. 2017. *Towards a fast and secure design for enterprise-oriented cloud storage systems*. Wiley. 1-15.

Edward A. P. MD, MPH. 2008. Survey-Based Research: General Principles. Basics of Research Part 9. *Air Medical Journal* 27:1, 14-16

Elnaggar, R., Basu, K., Chakrabarty, K. & Karri, R., 2021. Run-time Malware Detection Using Embedded Trace Buffers. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.

Fargo, F. & Sury, S. 2018, October. Autonomic Secure HPC Fabric Architecture. *In 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. 1-4.

Foreman, J.C., 2018. A Survey of Cyber Security Countermeasures Using Hardware Performance Counters. arXiv preprint arXiv: 1807-10868.

Gamblin, T. and Katz, D.S., 2022. Overcoming Challenges to Continuous Integration in HPC. *Computing in Science & Engineering*, *24*(6), pp.54-59.

González, Á. F, Rosillo, R., Dávila, J.Á. M & Olivera, V. M, 2015. Historical review and future challenges in Supercomputing and Networks of Scientific Communication. *The Journal of Supercomputing*, *71*(12): 4476-4503.

Harvard: Creswell, J.W., 2021. *A concise introduction to mixed methods research*. SAGE publications.

Hawkins, J.M. and Silva, B.C., 2018. Textual analysis. *The SAGE Encyclopedia of Communication Research Methods. Los Angeles, CA: SAGE Publications*.

Hanson, D. and Grimmer, M., 2007. The mix of qualitative and quantitative research in major marketing journals, 1993-2002. *European journal of marketing*.

Hopkins, W.G., 2000. Measures of reliability in sports medicine and science. *Sports medicine*, *30*(1), pp.1-15.

Hwang, I., Wakefield, R., Kim, S. and Kim, T., 2021. Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), pp.345-356.

Jungwirth, P., Chan, P., Barnett, T. & Badawy, A.H., 2018. Cyber defense through hardware security. In Disruptive Technologies in Information Sciences. *International Society for Optics and Photonics*. 10652: (106520P).

Jamshed, S., 2014. Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), p.87.

Jungwirth, P and La Fratta, P. 2017: *OS Friendly Microprocessor Architecture, Army Research Lab Report ARL-SR-0370*. http://www.arl.army.mil/arlreports/2017/ARL-SR-0370.pdf [24 June 2019]

Kamila, N.K., Pani, S.K., Bharti, P.K. and Sahoo, S., An Evolutionary Technical & Conceptual Review on High Performance Computing Systems.

Khessib, B., Kelly, B.D. & Bulusu, M., Microsoft Technology Licensing LLC, 2019. *Hardware-enforced firmware security*. U.S. Patent Application 15: 694-748.

Lincoln, Norman K. Denzin Yvonna S. *The Sage handbook of qualitative research*. Sage, 2005.

Leedy, P.D. and Ormrod, J.E. 2005. Practical Research: Planning and Design. Prentice Hall, Upper Saddle River, NJ. http://www.worldcat.org/title/practical-research-planning-and-design/oclc/53831701

Lisa M. Given. 2012. The SAGE Encyclopaedia of Qualitative Research Methods. *SAGE Publications, Inc.* 865-866

Li, K.C., Sukhija, N., Bautista, E. and Gaudiot, J.L. eds., 2022. *Cybersecurity and High-Performance Computing Environments: Integrated Innovations, Practices, and Applications*. CRC Press.

Messerli, A.J., Voccio, P. and Hincher, J.C., RACKSPACE US Inc, 2017. *Multi-level cloud computing system*. U.S. Patent 9: 563-480.

Mabakane, M.S., Moeketsi, D.M. & Lopis, A.S., 2017. Scalability of DL_POLY on high performance computing platform. *South African Computer Journal*, *29*(3), pp.81-94.

Mabakane, M.S., 2019. *Effective visualisation of callgraphs for optimisation of parallel programs: a design study* (Doctoral dissertation, Faculty of Science).

Maitra, S. and Madan, S., 2017. Intelligent Cyber Security Solutions through High Performance Computing and Data Sciences: An Integrated Approach. *IITM Journal of Management and IT*, *8*(1): 3-9.

Mildenberger, M., 2023. Security Infrastructures and intrusion systems.

Moore, D.S., Notz, W.I. and Notz, W., 2006. *Statistics: Concepts and controversies*. Macmillan.

Neuman, W.L., 2006. *Workbook for Neumann Social research methods: qualitative and quantitative approaches*. Allyn & Bacon.

Neuman, W.L., 2011. *Social Research Methods: Qualitative and Quantitative Approaches*, ed. 7th, 75 Arlington Street, Suite 300, Boston, MA 02116: Peaarson Education.

Nolte, H., Sabater, S.H.S., Ehlers, T. and Kunkel, J., 2022, May. A Secure Workflow for Shared HPC Systems. In *2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid)* (pp. 965-974). IEEE.

Nolte, H., Spicher, N., Russel, A., Ehlers, T., Krey, S., Krefting, D. and Kunkel, J., 2023. Secure HPC: A workflow providing a secure partition on an HPC system. *Future Generation Computer Systems*, *141*, pp.677-691.

Nosek, M. and Szczypiorski, K., 2022, January. An Evaluation of Meltdown Vulnerability. In *Proceedings of the 2022 9th International Conference on Wireless Communication and Sensor Networks* (pp. 35-41).

Kocher, P. Genkin, D. Gruss, D. Haas, W. Hamburg, M. L. Mangard, S. Prescher, T. Schwarz, M. & Yarom, Y. 2018. *Spectre Attacks: Exploiting Speculative Execution.* Cornell University Library. https://arxiv.org/pdf/1801.01203.pdf [14 May 2019]

Patton, M.Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Sciences Research, 34,* 1189–1208.

Pesämaa, O., Zwikael, O., HairJr, J. and Huemann, M., 2021. Publishing quantitative papers with rigor and transparency. *International Journal of Project Management*, *39*(3), pp.217-222.

Peisert, S. 2017. Security in High Performance Computing Environments. 60(9): 72-80, *Communications of the ACM*.

Patton, M.Q. "Enhancing the quality and credibility of qualitative analysis." *Health services research* 34, no. 5 Pt 2 (1999): 1189.

Pittalia, P.P., 2015. Advanced Security Policies to protect the Internet resources against the cyber attacks. *International Journal of Advanced Research in Computer Science*, *6*(6).

Ponce, M. and van Zon, R., 2023. Cybersecurity Training for Users of Remote Computing. *arXiv preprint arXiv:2306.07192*.

Rahman, M.M., Tabash, M.I., Salamzadeh, A., Abduli, S. and Rahaman, M.S., 2022. Sampling techniques (probability) for quantitative social science researchers: a conceptual guidelines with examples. *Seeu Review*, *17*(1), pp.42-51.

Sadiku, M.N.O., Sarhan, M.M. & Osama, M.M. 2017. High-Performance Computing: A Primer*. International Journal of Advanced Research in Science, Engineering and Technology,* 4(10): 4661-4662.

Shamsi, J.A., Zeadally, S. & Nasir, Z., 2016. Interventions in cyberspace: status and trends. *IT Professional*, *18*(1): 18-25.

Saunders, M., Lewis, P. and Thornhill, A., 2009. *Research methods for business students*. Pearson education.

Saunders, M., Lewis, P. and Thornhill, A., 2009. Understanding research philosophies and approaches. *Research methods for business students*, *4*(1), pp.106-135.

Singh, A. & Chatterjee, K. 2017 Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications,* 88-155.

Spalazzi, L. & Vigano, L. 2015. Special issue on security and high performance computing systems*. Journal of Computer Security,* 23: 539–540.

Stevens, S.S., 1946. On the theory of scales of measurement.

Torbet, G. 2019. https://www.makeuseof.com/tag/what-is-uefi-and-how-does-it-keep-you-more-secure/ [23 January 2020].

Varghese, B. & Buyya, R. 2017. *Next Generation Cloud Computing: New Trends and Research Directions.* Future Generation Computer Systems, 7 September 2017*.*

Vasilas, T., Jakobsche, T. and Ciorba, F.M., 2023, July. Hot-n-Cold: Mapping the Syscall Attack Surface Using Thermal Side Channels. In *2023 22nd International Symposium on Parallel and Distributed Computing (ISPDC)* (pp. 93-100). IEEE

Waghmare, V. & Kapse, S. 2016. *Authorized Deduplication: an Approach for Secure Cloud Environment.* International Conference on Information Security and *Privacy (ICISP2015).*

Welman, J. C., Kruger, S. J. 2005. Research Methodology for the Business and Administrative Sciences. 3rd edition. Cape Town: Oxford University Press.

Weaver, V.M., 2022, November. Improving HPC Security with Targeted Syscall Fuzzing. In *2022 IEEE/ACM First International Workshop on Cyber Security in High Performance Computing (S-HPC)* (pp. 1-8). IEEE.

Wahyuni, D., 2012. The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, *10*(1), pp.69-80.

Yellu, P., Zhang, Z., Monjur, M.M.R., Abeysinghe, R. & Yu, Q., 2019, September. Emerging Applications of 3D Integration and Approximate Computing in High-Performance Computing Systems: Unique Security Vulnerabilities. In *2019 IEEE High Performance Extreme Computing Conference (HPEC)* (pp. 1-7). IEEE.

Zhang, Z., Qi, J., Cheng, Y., Jiang, S., Lin, Y., Gao, Y., Nepal, S., Zou, Y., Zhang, J. and Xiang, Y., 2022. A Retrospective and futurespective of Rowhammer attacks and defenses on DRAM. *arXiv preprint arXiv:2201.02986*.

Zakhour, Z. 2017. *Develop a New HPC Cybersecurity Mindset. HPC Leading Edge.* http://www.digitaleng.news/de/develop-new-hpc-cybersecurity-mindset/ .[24 May 2018].

APPENDIX/APPENDICES

160

APPENDIX A: Questionnaire design

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only *Section 1, Question 1*. *Section 1, Question 1*
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
   . You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

* Indicates required question

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button below
to continue.

Demographics

1. 1. What is your occupation/role? *

Mark only one oval.

- ◯ Systems Administrator in an HPC environment.
- ◯ Security Administrator in an HPC environment.
- ◯ User in an HPC environment.
- ◯ I do not work in an HPC environment.
- ◯ Other: _____

Skip to question 2

Security breaches

2. 1. Indicate how many security breaches you have had in the last four years. *

Mark only one oval.

- 0 *Skip to question 16*
- 1
- Other: _____

3. 2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

Mark only one oval.

- Rootkit
- DDoS attack
- Backdoor
- Trojan horse
- Privilege escalation attack
- I dont know
- None
- Other:

4. 3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system. *Mark only one oval.*

- Rootkit
- DDoS attack
- Backdoor
- Trojan horse
- Privilege escalation attack
- I dont know
- None
- Other:

5. 4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system. *Mark only one oval.*

   - Rootkit
   - DDoS attack
   - Backdoor
   - Trojan horse
   - Privilege escalation attack
   - I dont know
   - None
   - Other:

6. 5. How was the **first** attack detected?

   Mark only one oval.

   - Monitoring tool
   - After compromise
   - An alert
   - Other:

7. 6. How was the **second** attack detected?

Mark only one oval.

- ◯ Monitoring tool
- ◯ After compromise
- ◯ An alert
- ◯ There was no second attack
- ◯ Other: _____

8. 7. How was the **third** attack detected?

Mark only one oval.

- ◯ Monitoring tool
- ◯ After compromise
- ◯ An alert
- ◯ There was no third attack
- ◯ Other: _____

9. 8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

Tick all that apply.

- ☐ Security Information and Event Management (SIEM)
- ☐ Endpoint Data loss Prevention (DLP)
- ☐ User behaviour intelligence tools
- ☐ User behaviour analytics tools
- ☐ User activity monitoring tools
- ☐ Other: _____

Compromised system

10. 1. What damage has been caused by the **first** attack which has managed to compromise the system?

Tick all that apply.

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other:

_____

11. 2. What damage has been caused by the **second** attack which has managed to compromise the system?

Tick all that apply.

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system There
- [ ] was no further attack
- [ ] Other:

_____

12. 3. What damage has been caused by the **third** attack which has managed to compromise the system?

Tick all that apply.

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other:

13. 4. How long has the **first** attack kept the system offline?

Mark only one oval.

- 1 day
- 2 days
- 3 days
- 4 days
- 5 Other:

14. 5. How long has the **second** attack kept the system offline?

Mark only one oval.

- 1 day
- 2 days
- 3 days
- 4 days
- There were no more than three attacks
- Other:

15. 5. How long has the **third** attack kept the system offline?

Mark only one oval.

- 1 day
- 2 days
- 3 days
- 4 days
- 5 Other:

HPC environment vulnerabilities

16. 1. What are some of the challenges you encounter in protecting your HPC system?

17. 2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

18. 3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

APPENDIX B: COLLECTED DATA

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ○ Systems Administrator in an HPC environment.
- ○ Security Administrator in an HPC environment.
- ○ User in an HPC environment.
- ◉ I do not work in an HPC environment.
- ○ Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ○ 0
- ○ 1
- ○ Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: _____

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: _____

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other:

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ( ) 0
- (●) 1
- ( ) Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- (●) Rootkit
- ( ) DDoS attack
- ( ) Backdoor
- ( ) Trojan horse
- ( ) Privilege escalation attack
- ( ) I dont know
- ( ) None
- ( ) Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ◉ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ◉ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ◉ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ◉ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ◉ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [x] Security Information and Event Management (SIEM)
- [x] Endpoint Data loss Prevention (DLP)
- [x] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [x] Compromise user data
- [x] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [x] Blocking legitimate users
- [x] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [x] Damage the system
- [x] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- (•) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ◉ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ◉ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

iuyiouyuioy

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

m;;'lkj;jk;'k;lk;lk;l

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

jlk;jk;ljkl;

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- (●) 0
- ( ) 1
- ( ) Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- (●) Rootkit
- ( ) DDoS attack
- ( ) Backdoor
- ( ) Trojan horse
- ( ) Privilege escalation attack
- ( ) I dont know
- ( ) None
- ( ) Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- (●) Rootkit
- ( ) DDoS attack
- ( ) Backdoor
- ( ) Trojan horse
- ( ) Privilege escalation attack
- ( ) I dont know
- ( ) None
- ( ) Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- (●) Rootkit
- ( ) DDoS attack
- ( ) Backdoor
- ( ) Trojan horse
- ( ) Privilege escalation attack
- ( ) I dont know
- ( ) None
- ( ) Other: .....

5. How was the **first** attack detected?

- (●) Monitoring tool
- ( ) After compromise
- ( ) An alert
- ( ) Other: .....

6. How was the **second** attack detected?

- (●) Monitoring tool
- ( ) After compromise
- ( ) An alert
- ( ) There was no second attack
- ( ) Other: .....

7. How was the **third** attack detected?

- (●) Monitoring tool
- ( ) After compromise
- ( ) An alert
- ( ) There was no third attack
- ( ) Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [x] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [x] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [x] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [x] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- (•) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) Other: .....

5. How long has the **second** attack kept the system offline?

- (●) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) There were no more than three attacks
- ( ) Other: .....

5. How long has the **third** attack kept the system offline?

- (●) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) Other: .....

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

hlhjlkhlkj

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

hlhjlkjlk;

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

kjhgjkhgjhk

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ( ) 0
- ( ) 1
- (●) Other: 5

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ◉ I dont know
- ○ None
- ○ Other: _____

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ◉ I dont know
- ○ None
- ○ Other: _____

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ◉ Other: ssh daemon

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1. What are some of the challenges you encounter in protecting your HPC system?

I dont know HOW-TO with the tools to deploy to monitoring and protect HPC System

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

Using Open sources tools to monitoring the clusters

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ○ Systems Administrator in an HPC environment.
- ○ Security Administrator in an HPC environment.
- ○ User in an HPC environment.
- ○ I do not work in an HPC environment.
- ◉ Other: Management in HPC

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ○ 0
- ○ 1
- ○ Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

Cyber attacks, illicit usage, power surged

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

1. Cyber attacks, 2. Unauthorised access, 3. Data storage safety

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1. Network management security
2. Authentication management
3. Storage level aunthenrication

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ○ Systems Administrator in an HPC environment.
- ◉ Security Administrator in an HPC environment.
- ○ User in an HPC environment.
- ○ I do not work in an HPC environment.
- ○ Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ◉ 0
- ○ 1
- ○ Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [x] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [x] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ◯ 1 day
- ◯ 2 days
- ◯ 3 days
- ◯ 4 days
- ◯ There were no more than three attacks
- ◯ Other: _____

5. How long has the **third** attack kept the system offline?

- ◯ 1 day
- ◯ 2 days
- ◯ 3 days
- ◯ 4 days
- ◯ Other: _____

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

Due to the collaborative nature of HPC research and the involvement of various users, insider threats is a significant concern. Users with legitimate access misuse their privileges.lack of Multi Factor

Authentication is also a challenge as the users only use ssh to authenticate to the system.Opening of various ports also pose a high risk to the HPC System which are requested by various HPC researchers.

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

1,Human errors, such as using weak passwords, sharing credentials, or inadvertently exposing sensitive data
2,Service like SSH, running on HPC systems may have vulnerabilities if not properly configured or patched.
3,Vulnerabilities in job schedulers used to manage and distribute computing tasks across nodes can be targeted for privilege escalation and unauthorized access.
4,Incorrectly configured systems, and network settings, can create vulnerabilities
5,High-speed interconnects used in HPC clusters, like InfiniBand, may have vulnerabilities in their firmware or software stacks

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1,Regular security audits and reviews can help identify and rectify misconfigurations.
2,Security awareness and training are important for mitigating these risks.
3,Regular patching and updates are essential to address these vulnerabilities.
4,Implementing strong access controls and monitoring user activities.

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ( ) 0
- ( ) 1
- (●) Other: We have not experienced any security breaches on our HPC system.

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ◉ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ◉ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ◉ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [x] Other:
  No attack or breach has occurred in the last four years. However, we have implemented proactive security measures, including the adoption of security tools and techniques (Network Filtering, Network Isolation, Activity Monitoring, Security Information and Event Management (SIEM), etc).

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

Challenges in safeguarding our HPC system include complexity, evolving threats, user access control, resource constraints, performance impact, data privacy compliance, patch management, and mitigating insider threats.

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

Vulnerabilities in HPC systems include complex architecture, evolving cyber threats, access control management, resource limitations, data privacy compliance, patch management, and potential insider threats.

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

To address the vulnerabilities in HPC systems, the best solutions are: (1) Implement robust access control measures to restrict unauthorized access;

(2) Stay updated on evolving cybersecurity threats through continuous monitoring; (3) Educate users to enhance their awareness of security best practices; (4) Allocate sufficient resources to bolster security measures; (5) Ensure timely updates and patch management for system components; (6) Employ behavior monitoring tools to detect unusual activities; (7) Develop a comprehensive strategy to mitigate insider threats effectively.

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ○ Systems Administrator in an HPC environment.
- ○ Security Administrator in an HPC environment.
- ◉ User in an HPC environment.
- ○ I do not work in an HPC environment.
- ○ Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ○ 0
- ○ 1
- ◉ Other: I'm not sure, sys admin staff handle it.

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

As a user I don't know but we wouldn't like an attack that deleted our data either through targeting our users or just indiscriminate deletion.

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

1. Probably, the demands for services and network access needs by the users do not know of or consider system security.

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1. Open communication between sys admin, users and system security as to risks from their usage and requirements.

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- (●) 0
- ( ) 1
- ( ) Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ◉ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: _____

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ◉ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ◉ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ◉ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ◉ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ◉ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [x] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [x] Compromise user data
- [x] Abuse of resources
- [ ] Blocking legitimate users
- [x] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [x] Compromise user data
- [x] Abuse of resources
- [ ] Blocking legitimate users
- [x] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [x] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- (•) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) Other: .....

5. How long has the **second** attack kept the system offline?

- (●) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) There were no more than three attacks
- ( ) Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ◉ Other: none

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

lack of security skills

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

i don't know

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

staying up to date/ alert with HPC vulnerables and create patches to avoid the exploitation of that said vulnerability

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- (●) Systems Administrator in an HPC environment.
- ( ) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ( ) 0
- ( ) 1
- (●) Other: 3

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ◉ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- (●) Rootkit
- ( ) DDoS attack
- ( ) Backdoor
- ( ) Trojan horse
- ( ) Privilege escalation attack
- ( ) I dont know
- ( ) None
- ( ) Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ◉ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ◉ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ◉ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ◉ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [x] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [x] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [x] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [x] Other: none

4. How long has the **first** attack kept the system offline?

- (•) 1 day
- ( ) 2 days
- ( ) 3 days
- ( ) 4 days
- ( ) Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ◉ Other: 0

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ◉ Other: 0

HPC environment vulnerabilities

1. What are some of the challenges you encounter in protecting your HPC system?

Inadequecy of tools addressing data loss (Data integrity)

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

1. Weak authentication policies leading to the success of brute force attacks 2. Absence of Configuration Management tools for consistency

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

MFA and puppet

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ○ Systems Administrator in an HPC environment.
- ○ Security Administrator in an HPC environment.
- ○ User in an HPC environment.
- ○ I do not work in an HPC environment.
- ◉ Other: Scientist

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ○ 0
- ○ 1
- ○ Other: _____

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1. What are some of the challenges you encounter in protecting your HPC system?

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).

HPC System breaches

1. This questionnaire is to be completed by an employee working in an HPC environment.
2. If you have not been working with HPC systems, complete only ***Section 1, Question 1***.
3. The purpose of this questionnaire is to investigate the types of breaches that occur in a High Performance Computing (HPC) systems.
4. This questionnaire has 18 questions and should take no more than 10 minutes to complete.
5. Contact the researcher for any inquiries about this survey: zintle.sanda@gmail.com
6. You are requested to please complete and submit this survey by **25 October 2023, 16:00 pm SAST.**
7. This questionnaire forms part of a Masters study in the IT department at the Cape Peninsula University of Technology: *Classifying High Performance Computing system breaches and finding common trends*.

Informed consent:

a) Participants in this survey are assured that all information received will be treated as strictly confidential.

b) Participation in this survey is voluntary.

c) This survey is completely anonymous - your identity is not required, and even if you supply it, it will not be divulged to any other person or company in any way.

d) All responses will be used for academic purposes and none of your details will be provided to any other person or company other than the researcher and her study leader.

Thank you.

Please click on the "Next" button
below to continue.

Demographics

1. What is your occupation/role? *

- ( ) Systems Administrator in an HPC environment.
- (•) Security Administrator in an HPC environment.
- ( ) User in an HPC environment.
- ( ) I do not work in an HPC environment.
- ( ) Other: _____

Security breaches

1. Indicate how many security breaches you have had in the last four years. *

- ( ) 0
- ( ) 1
- (•) Other: More than the organisation is aware of

2. Complete this question only if you had **one** of the following security attacks or breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

3. Complete this question only if you had **a second one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

4. Complete this question only if you had **a third one** of the following security attack and breach in the last four years? Please select which breach you have seen on your system.

- ○ Rootkit
- ○ DDoS attack
- ○ Backdoor
- ○ Trojan horse
- ○ Privilege escalation attack
- ○ I dont know
- ○ None
- ○ Other: .....

5. How was the **first** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ Other: .....

6. How was the **second** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no second attack
- ○ Other: .....

7. How was the **third** attack detected?

- ○ Monitoring tool
- ○ After compromise
- ○ An alert
- ○ There was no third attack
- ○ Other: .....

8. In the last four years, what have been the tools used to identify or protect against a potential **insider attack** targeting the system?

- [ ] Security Information and Event Management (SIEM)
- [ ] Endpoint Data loss Prevention (DLP)
- [ ] User behaviour intelligence tools
- [ ] User behaviour analytics tools
- [ ] User activity monitoring tools
- [ ] Other: .....

Compromised system

1. What damage has been caused by the **first** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] Other: .....

2. What damage has been caused by the **second** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There was no further attack
- [ ] Other: .....

3. What damage has been caused by the **third** attack which has managed to compromise the system?

- [ ] Compromise user data
- [ ] Abuse of resources
- [ ] Blocking legitimate users
- [ ] Damage the system
- [ ] There were no more than three attacks
- [ ] Other: .....

4. How long has the **first** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: .....

5. How long has the **second** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ There were no more than three attacks
- ○ Other: _____

5. How long has the **third** attack kept the system offline?

- ○ 1 day
- ○ 2 days
- ○ 3 days
- ○ 4 days
- ○ Other: _____

HPC environment vulnerabilities

3. In your opinion, what could be the best solution/s to address these vulnerabilities? (Please number them according to above).

1. What are some of the challenges you encounter in protecting your HPC system?

2. In your opinion, what are the vulnerabilities currently in HPC systems? (Please number them).