Science, Engineering & Education, 9, (1), 2024, 3-12

From Firewall to AI: Strengthening Linux Server Security

Ivaylo Atanasov*

University of Chemical Technology and Metallurgy, 8 Kliment Ohridski Blvd., Sofia 1797, Bulgaria

Received 13 March 2024, Accepted 21 October 2024
DOI: 10.59957/see.v9.i1.2024.1

ABSTRACT

Nowadays, cybersecurity issues are constantly increasing. Some of the main challenges are the rapidly evolving threat landscape, the lack of skilled cybersecurity professionals, complexity of IT environments and emerging technologies, Zero-Day vulnerabilities, lack of international cooperation, user behavior and social engineering. The selection of an operating system can significantly influence the establishment of robust defenses against cyber threats. Now, many strategies are known for defense-in-depth of critical server infrastructure, but the ever-increasing sophistication of cyber-attacks must also be considered. When a previously unknown attack occurs, a defense system must be able to recognize it and act. The current development of Artificial Intelligence (AI) makes it possible to create this type of intelligent protection. This paper aims to provide an overview of some of the most renowned traditional practices and explores the potential of leveraging a neural network model to enhance cybersecurity used to protect Linux servers against cyber-attacks.

Keywords: cybersecurity, linux server, artificial intelligence, artificial neural networks.

INTRODUCTION

While there exist numerous methods for infiltrating an IT system, most cyber-attacks depend on similar techniques. Listed below are some of the most common attacks: Malware like Ransomware, Spyware, Trojan horses, Viruses, Adware and Cryptojacking; Spoofing; Phishing Attacks; Distributed Denial-of-Service (DDoS) Attacks; SQL Injection; Man-in-the-middle attack (MITM); Zero-day Exploit and IoT-Based Attacks; DNS Tunneling; Session Hijacking Attacks; Cross-Site Scripting (XSS) Attacks; Password Attacks like Brute Force Attack; Insider Threats; Identity Theft; Advanced Persistent Threat (APT) and Drive-by Attacks.

The Role of Linux in Enhancing the Security of Digital Infrastructure

Global cyberattacks increased by 38 % in 2022 compared to 2021 [1]. According to W3Cook‘s examination of Alexa‘s data, Linux powers an overwhelming 96.3 % of the top 1 million web servers. The remaining market share is divided between Windows, accounting for 1.9 %, and FreeBSD, with 1.8 % [2]. Therefore,

**Correspondence to: Ivaylo Atanasov, University of Chemical Technology and Metallurgy*
8 Kliment Ohridski Blvd., Sofia 1797, Bulgaria, E-mail: ivaylo@uctm.edu

it is extremely important to ensure that Linux Servers have adequate protection against cyber-attacks. Linux or GNU/Linux is the common name for all operating systems, based on the Linux kernel and system tools and libraries, usually from the GNU project. Most of these operating systems are called Linux distributions, but the Free Software Foundation uses the name GNU/Linux, to emphasize the importance of GNU software, which causes some controversy. Linux is the flagship and one of the best-known representatives of free software and open-source software (F(L)OSS - Free/Libre and open-source software). Linux has emerged as the prevailing operating system for servers, mainframes, and even supercomputers. Notably, since 2017, all the top 500 fastest supercomputers have adopted Linux-based operating systems exclusively [3 - 5]. Linux is often regarded as more secure than other operating systems due to its reduced susceptibility to various malware forms, for instance ransomware, backdoors, computer viruses, spyware, worms, Trojan horses, rogue software, keyloggers, etc. However, software vulnerabilities also exist in Linux. By design Linux prioritizes security with various features like process isolation, privilege separation and fine-grained access controls through Access Control Lists (ACL's) but also although difficult to implement Mandatory Access Control (MAC) like SELinux, SMAC, AppArmor, TOMOYO, etc. These security mechanisms provide a robust basis in enhancing the security of digital infrastructure.

Enhancing Linux security with The Linux Security Modules (LSM)

Common vulnerabilities found in Linux systems include privilege escalation, memory corruption, and information disclosure. These vulnerabilities can be exploited by hackers to gain unauthorized access to a Linux server and steal or destroy data. The Linux Security Modules (LSM) aims to address this challenge by offering a framework for security policy modules and access control mechanisms. The LSM framework provided on Fig. 1 has a modular architecture that incorporates embedded hooks within the kernel, facilitating the installation of security modules designed to strengthen access control. Mandatory Access Control (MAC) extensions, which establish comprehensive security policies, are the principal users of the LSM interface. MAC systems such as SELinux are designed and developed as LSM modules [6].

A list of the active Linux Security Modules can be found by reading /sys/kernel/security/lsm. Activated Linux Security Modules in Debian 12 GNU/Linux standard installation:

```
lockdown,capability,landlock,yama,apparmor,tomoyo,bpf
```

Activated Linux Security Modules in Alma Linux 8.8 standard installation:

```
capability,yama,selinux,bpf
```

Advantages of LSMs

Enhanced security; fine-grained access control; isolation; application sandboxing (Apparmor); policy customization; logging and auditing; community support.

Disadvantages of LSMs

Complexity; compatibility issues; false positives; performance overhead.

OpenSSH Server Security Hardening

Open Secure Shell (OpenSSH) is a widely used open-source implementation of the SSH (Secure Shell) protocol. SSH is a network protocol that provides secure encrypted communication between two computers over an insecure network, typically to securely log into remote systems and execute commands. Hardening the default configuration that comes with the standard installation is done to eliminate the possibility of someone getting sensitive data or unauthorized access using various network attacks. Some aspects of OpenSSH hardening

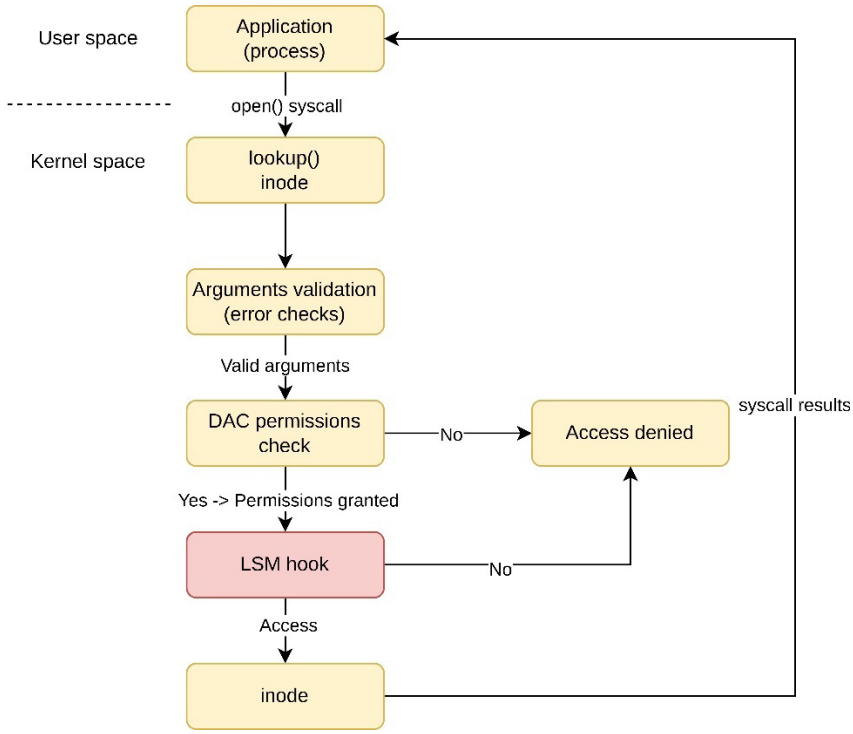

Fig. 1. Linux Security Modules Framework.

include these steps:

- Changing the Default SSH Port
- Disabling passwords logins.
- Disabling root user login
- Creating and managing keys for passwordless logins
- Configuring Secure Shell with strong encryption algorithms
- Access control with whitelists and TCP Wrappers Hardening
- Configuring automatic logouts
- Disabling X11 Forwarding and SSH Tunneling (SSH Port Forwarding)
- Configuration of access control directives
- Creation of pre-login security banners

Access Control Lists (TCP wrappers)

TCP Wrappers is a host-based networking ACL system for restricting access to TCP services based on defined ACLs (Access Control Lists) based on hostname, IP address, network address, etc. To determine whether a client machine is allowed to connect to SSH, TCP Wrappers refer to the following two files, commonly referred to as host access files:

- /etc/hosts.allow
- /etc/hosts.deny

When a client request is received by TCP Wrappers, it undertakes the following algorithm:

It sequentially parses the /etc/hosts.allow file and applies the first rule specified for this service. If it finds a matching rule, it allows the connection. If not, it proceeds to sequentially parsing /etc/hosts.deny, where if a matching rule is found to be set, the connection is terminated. Otherwise, access to the service is granted.

Access rules in hosts.allow are applied first and take precedence over rules specified in hosts.deny. If access to a service is allowed in hosts.allow, a rule denying access to the same service in hosts.deny is ignored. The order of the rules is extremely important because the rules in each file are read from top to bottom and the first matching rule for a given service is the only one

that applies. TCP Wrappers do not cache rules from host access files, and any changes to hosts. allow or hosts.deny take effect immediately without restarting network services. If no service rules are found in any file, or if none exist, access to the service is granted. For this reason, the recommended setting is to deny anything that is not explicitly allowed.

Advantages of TCP wrappers

Straightforward way to control access to network services; service-level control, flexibility, logging, protection from unauthorized access; compatibility.

Disadvantages of TCP wrappers

Limited to network services; not a complete security solution; potential for false positives; TCP wrappers by themselves, do not offer encryption or authentication mechanisms; complexity for complex policies; dependent on network information - can be bypassed by spoofing ACLs based on IP addresses or hostnames.

Firewall

The firewall is specialized hardware or software that inspects network traffic passing through it and allows or denies access according to certain rules. Most often, firewalls work at the level of the network and transport layers (network layer, transport layer), where they examine the data packets of the TCP and IP (Transmission Control Protocol, Internet Protocol) protocols and usually make their decisions depending on the IP address of the sender or the destination port from which the packet was received or to which it will be sent, or any combination of these parameters. Options in the package header are also analyzed. Firewalls, which operate at the application layer of the Open Systems Interconnection (OSI) model, filter traffic between internal and external networks in terms of the information carried in the packets, using set keywords, and watching for spam, computer viruses and Trojan horses.

Linux netfilter

The Linux kernel includes the netfilter subsystem, which is used to manipulate or decide the processing of network traffic directed to, from, or through the computer. All modern Linux firewall solutions use this packet filtering system. The kernel's packet filtering system would be useless to users or administrators without a user interface to manage it. This is the purpose of nftables, which serve as replacements for iptables, ip6tables, arptables, ebtables, and ipset. When a packet reaches a computer, it passes to the netfilter subsystem to accept, manipulate, or reject based on the rules provided to it via nftables. nftables is a database of firewall rules and is the actual firewall used on Linux systems. The traditional interface for configuring nftables on Linux systems is the nftables interface terminal on the command line. The other utilities like ufw and firewalld simplify the manipulation of the nftables database. Although nftables is a robust and flexible tool, configuring the firewall via the CLI would be time-consuming even for experts.

Advantages of netfilter

Advanced features; stateful inspection, custom rules, logging; integration into the linux kernel; low-level access to network packets; security.

Disadvantages of netfilter

Complex configuration; potential for misconfiguration; limited user-friendliness.

The default firewall configuration tool for Ubuntu Server is Uncomplicated Firewall (UFW). UFW is designed to simplify the configuration of nftables, providing an intuitive method for creating host-based firewalls for both IPv4 and IPv6 networks. By default, ufw is disabled. [7]. For Red Hat Enterprise Linux (RHEL) and its derivatives, firewalld is a firewall service daemon (frontend controller for nftables) that offers a dynamic and customizable host-based firewall with a D-Bus interface. Its dynamic nature allows

for the creation, modification, and deletion of rules without requiring a restart of the firewall daemon each time rules are altered [8,9].

Port Knocking

Port Knocking is a method of allowing access to ports (services, applications) that are by default prohibited in the firewall [10]. Its purpose is to implement an additional level of port protection. This is suitable for services such as SSH, RDP, L3 Virtual Private Network (VPN), etc. Typically, access is granted after performing a strict sequence of taps - sending TCP or User Datagram Protocol (UDP) packets to specific port numbers (from 1 to 65535). TCP and UDP are most often used, but it is possible to implement the method both through protocols of a lower level than the transport level, and at a higher level - for example Application layer (Layer 7).

Main advantages of the Port knocking:

Increasing the security of certain services; authentication through the firewall resources; temporarily establishing a connection through closed ports; great dynamics and a rich variety of combinations; lack of a mechanism to check whether "port tapping" is implemented.

Disadvantages of the Port knocking:

Systems lacking cryptographic hashes are susceptible to IP address spoofing attacks; port knocking can pose challenges in networks with significant latency; single point of failure if - the failure of the Port knocking daemon will deny port access to all users although modern implementations address this problem by including a process-monitoring daemon capable of restarting a port knocking daemon process that has failed or become stuck.

Intrusion Prevention System (IPS)

fail2ban is a popular Intrusion Prevention System (IPS) that protects Linux servers and blocks brute-force and other automated attacks by analyzing system logs using regular expressions for suspicious activity. If the number of attacks exceeds a certain predefined level, fail2ban blocks the corresponding IP through the system firewall for a certain period.

Advantages of fail2ban

Enhanced security, Flexible configuration, Ease of use for basic use cases, Log monitoring, Adaptive blocking; Logging and notifications.

Disadvantages of fail2ban

Configuration complexity; false positives, resource usage, limited protection against sophisticated attacks; logging overhead; work only with network services.

Other Basic Measures to Increase Defense Against Cyber Attacks for Linux Servers

The following practices, widely recognized and renowned for their effectiveness in enhancing the security of Linux servers, are listed here:

- Manage file permissions with Discretionary Access Control (DAC)
- Keep software up to date with automatic security updates
- Disable unwanted Linux services via systemctl
- Monitor server logs
- Disable unwanted Set-User-ID (SUID) and Set-Group-ID (SGID) binaries
- Harden the Linux kernel
- Regular backups
- Network segmentation and isolation
- Encryption to protect confidential information and encryption of communications
- Two-Factor Authentication
- Separate disks partition
- Disks quotas
- Malware and vulnerability scanners
- Restricting sudo users
- Password aging
- Locking user accounts after login failure

- Secure web servers
- Database security
- Running services in containers
- Eliminate single points of failure with High Availability (HA)

Intelligent Methods for Cybersecurity

Because cyber-attacks are not static, but rather continuously evolving, an intelligent system can be designed with an AI-based protection to detect previously unknown cyber-attacks.

In recent years Cybersecurity has benefited from the rapid development of AI. Listed below are some modern methods that may be implemented to protect against cyber-attacks:

- System behaviors analysis with machine learning
- User and entity behavior analytics
- AI-driven vulnerability assessment
- Real time network traffic analysis based on AI
- Adaptive access control
- Deep Learning for malware detection
- AI-enhanced Intrusion detection and prevention
- Predictive analysis with AI algorithms
- Continuous learning and improvement of existing models

In response to the ever-evolving cyber threats and the increasing complexity of digital technologies, it is imperative that we invest in the development of well-known and widely used cybersecurity frameworks like NIST Cybersecurity Framework [11].

Intelligent methods for cybersecurity on Linux servers show the potential of AI in enhancing security by proactively identifying, mitigating, and responding to threats in a dynamic and efficient manner. AI-driven solutions have broad applications in the realm of cybersecurity across multiple domains, encompassing endpoint security, application security, IoT security, web security, security operations and incident response, threat intelligence, mobile security, cloud security, network security, and human security [12].

Physical security is also critical, particularly in safeguarding server rooms. Integrating physical and digital elements in cyber-physical systems plays a crucial role in protecting sensitive infrastructure [13]. This integration is especially important for securing data centers, server rooms, and small businesses. It may involve incorporating pre-trained neural network models into physical cybersecurity systems, which typically feature video surveillance with integrated Convolutional Neural Networks (CNN) [14], additional sensors, database, data representation, and decision-making processes [15]. AI has the potential to significantly enhance cybersecurity efforts, but it also presents negative aspects that make it a double-edged sword. AI systems can be vulnerable to adversarial attacks, where malicious actors manipulate or trick AI algorithms into making incorrect decisions. This can be particularly dangerous in security applications, as attackers could exploit AI systems to bypass defenses. Several other negative aspects include data bias, privacy and ethical concerns, regulatory and legal challenges, and more [16].

Artificial Neural Networks (ANN) can be trained on vast datasets encompassing network traffic logs, IDS/IPS alerts, file audit logs, vulnerability scanner reports, rootkit scanners and other security-related data. This data can also include hardware metrics such as CPU temperature, utilization levels, memory usage, and storage performance. The data generated from these established security methods can be harnessed as valuable input for AI-based adaptive security solutions. By incorporating this additional data, the ANN can not only identify suspicious network activity but also detect potential threats based on unusual hardware behavior. For instance, a sustained spike in CPU temperature or memory usage could indicate unauthorized resource consumption, alerting security personnel

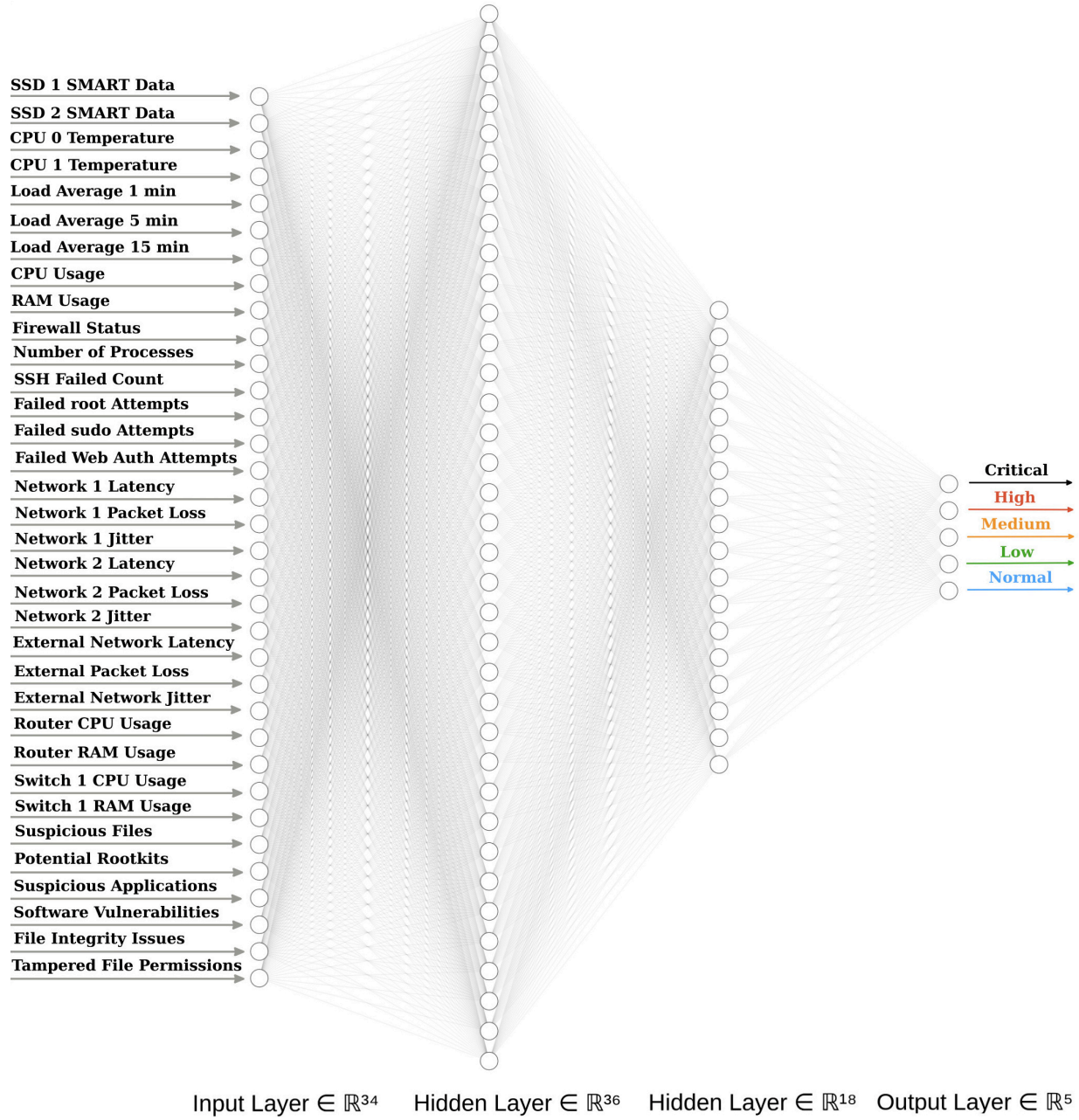

Fig. 2. Neural network model.

to investigate. This comprehensive data feed allows the ANN to learn complex patterns and identify subtle anomalies indicative of potential threats. This allows the AI system to categorize threats based on severity (low, medium, high, critical) and trigger automated responses, such as isolating infected systems or blocking malicious traffic. The neural network is currently under development and schematic depiction of the can be found in Fig. 2.

The development of such a model hinge on the creation of a comprehensive cybersecurity dataset for effective training.

Database Selection for Efficient Storage

Time-series databases (TSDBs) are particularly well-suited for storing the security data collected. TSDBs are optimized for handling

high-volume data streams with timestamps, allowing for efficient storage and retrieval of the security readings over time. This enables the AI model to access historical data for trend analysis and to train on a broader range of security scenarios.

Continuous Learning and Improved Security

As the AI model is exposed to new data over time, it continuously learns and refines its ability to detect threats. This continuous learning cycle is crucial for keeping pace with the ever-evolving threat landscape. By leveraging the rich data collected from the various parameters and stored effectively in a TSDB, AI-powered security solutions can become more proficient in safeguarding critical IT infrastructure.

A custom-designed software program acts as a central hub, continuously feeding the collected security data into a time-series database. This TSDB is specifically designed to efficiently store and manage high-volume, timestamped data streams. Fig. 3 illustrates the various data parameters obtained from Virtual Data Center environment based on GNU/Linux that serve as inputs for the neural network. The software program can also be used to display parameters

```
RAM Usage: 27.74%
Node1 Firewall: 1
Number of Processes: 781
All Failed SSH Connection Attempts (Last 10 minutes): 1
Privilege Escalation (sudo) Authentication Failure Activity (Last 10 minutes): 0
Network1 Latency Avg (ms): 0.089
Network1 Packet Loss (%) : 0%
Network1 Jitter (ms): 0.034
Network2 Latency Avg (ms): 0.224
Network2 Packet Loss (%) : 0%
Network2 Jitter (ms): 0.016
External Network Latency Avg (ms): 1.261
External Network Packet Loss (%): 0%
External Network Jitter (ms): 0.107
Network Device ID 1 CPU Load: 1 %
Network Device ID 1 Memory Percentage: 59 %
Network Device ID 2 CPU Load: 2 %
Network Device ID 2 Memory Percentage: 9 %
Network Device ID 3 CPU Load: 0 %
Network Device ID 3 Memory Percentage: 12 %
Rkhunter Malware Scan - Suspect files: 9
Rkhunter Malware Scan - Possible rootkits: 0
Rkhunter Malware Scan - Suspect applications: 0
Feb 2 09:19:56] INFO [localhost] pve-node1: Known Exploited Vulnerabilities are detected for 0 CVEs : 0
Feb 2 09:19:57] INFO [localhost] pve-node2: Known Exploited Vulnerabilities are detected for 0 CVEs : 0
Feb 2 09:19:57] INFO [localhost] pve-node3: Known Exploited Vulnerabilities are detected for 0 CVEs : 0
Number of nodes in cluster: 3
Ceph Status: HEALTH_OK : 1
Time difference between 192.168.1.41 and 192.168.1.42: 518 µs
Time difference between 192.168.1.42 and 192.168.1.43: 391 µs
Time difference between 192.168.1.41 and 192.168.1.43: 128 µs
Changed critical files: 2
Changed permissions of critical files: 32
Cybersecurity Incidents in the Last Hour [Severity: [Score ]: 4
Cybersecurity Incidents in the Last Hour [Severity: [Susp ]: 194
Cybersecurity Incidents in the Last Hour [Severity: [Blacklisted ]: 3
```

Fig. 3. Part of inputs for the neural network.

in real-time. While the challenge of acquiring sufficient training data exists, the development of comprehensive cybersecurity datasets is actively progressing, paving the way for future implementation.

CONCLUSIONS

The integration of traditional protection practices together with AI-based ones leads to improved accuracy, reduced response time and enhanced threat detection capabilities. By combining the strengths of traditional security measures with the adaptability of AI, organizations can better safeguard their valuable data. This approach fortifies defenses against known threats and equips systems to identify and respond to emerging and previously unseen cyber threats.

In the ongoing battle to protect against cyber threats, the synergy between traditional and AI-driven defenses is crucial. However, it is essential to address the potential drawbacks, including the possibility of false alarms and excessive reliance on AI. To mitigate these risks, organizations should regularly update their AI models, provide ongoing training for their cybersecurity teams, and maintain an adaptable security strategy that combines the strengths of traditional methods and AI-driven defenses. This multi-faceted approach ensures resilient and comprehensive protection against the ever-changing landscape of cyber threats.

REFERENCES

1. Gmcdouga, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks, Checkpoint, Available 2023.
2. S. Vaughan-Nichols, Can the Internet exist without Linux, https://www.zdnet.com/home-and-office/networking/can-the-internet-exist-without-linux, First Available 2015.
3. Linux and the GNU System, https://gnu.org, Available 2024.
4. R. Stallman, GNU/Linux FAQ, https://www.gnu.org/gnu/gnu-linux-faq.html, Available 2024.
5. TOP500 Supercomputers, https://en.wikipedia.org/wiki/TOP500, Available 2023.
6. C. Wrigh, C. Cowan, J. Morris, S. Smalley, Linux Security Module Framework, Ottawa Linux Symposium, 2002, Ottawa Canada.
7. J. LaCroix, Mastering ubuntu server - fourth edition: Explore the versatile, powerful linux server distribution Ubuntu 22.04 with this comprehensive guide, Packt, UK, 2022, p. 505.
8. Chapter 47, Using and configuring FIREWALLD Red Hat Enterprise Linux 8, https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/using-and-configuring-firewalld_configuring-and-managing-networking, Available 2024.
9. F. Houbart, Configure a firewall with FIREWALLD, Linode Guides, Available: https://www.linode.com/docs/guides/introduction-to-firewalld-on-centos, Available 2023.
10. P. Lunsford, E. Wright, Closed port authentication with Port Knocking, Annual Conference Proceedings, 2005, Portland, Oregon.
11. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, Available 2024.
12. P. Vähäkainu, M. Lehto, Artificial Intelligence and Cybersecurity Theory and Applications, Springer, Berlin, 2023, 3-27.
13. O. Tushkanova, D. Levshun, A. Branitsky, E. Fedorchenko, E. Novikova, I. Kotenko, Detection of cyberattacks and anomalies in cyber-physical systems: Approaches, data sources, evaluation, Algorithms, 16, 2, 85, 2023, 4-21.
14. L. Alzubaidi, J. Zhang, A.J. Humaidi, Review of deep learning: concepts, CNN architectures, challenges, applications, future directions, J. Big Data, 8, 53, 2021, 53.

15. I. Atanasov, D. Pilev, Cyber-physical security through facial recognition and sensor data analysis, J. Chem. Technol. Metall., 59, 2, 2024, 465-472.

16. M. Taddeo, T. McCutcheon, L. Floridi, Trusting artificial intelligence in cybersecurity is a double-edged sword, Nature Machine Intelligence, 1, 12, 2019, 557-560.