Article

Not peer-reviewed version

Automated Policy Violation Detection in Network Security Using Blockchain Technology

Syed Wasif Abbas Hamdani and Zia Muhammad *

Posted Date: 13 May 2025

doi: 10.20944/preprints202505.1028.v1

Keywords: Blockchain; Cybersecurity; Network Security; Automated Detection; Threat Detection; Smart Contracts; Policy Compliance; Enterprise Security; Security Auditing; Digital Forensics; Network Traffic Monitoring; Advanced Threat Detection; Real-time Network Monitoring; Network Traffic Analysis; Decentralized Verification.

 doi:10.20944/preprints202505.1028.v1

Article

Automated Policy Violation Detection in Network Security Using Blockchain Technology

Syed Wasif Abbas Hamdani [1] and Zia Muhammad [2,*]

[1] National University of Sciences and Technology (NUST), Islamabad, 46000, Pakistan
[2] Department of Computing, Design, and Communication, University of Jamestown, Jamestown, ND 58405, USA
* Correspondence: zia.muhammad@uj.edu

Abstract: For organizations with digital infrastructures, network security is crucial for mitigating potential cyber-attacks. Organizations establish security policies to protect systems and data, but employees may intentionally or unintentionally bypass these policies, rendering the network vulnerable to internal and external threats. Detecting these policy violations is challenging, requiring frequent manual system checks for compliance. This paper proposes a comprehensive set of advanced features for a modern network scanner, enhanced by blockchain technology, to automate and improve the analysis and detection of policy violations within organizations. While existing network scanners offer basic security checks such as firewall status, shared directory analysis, OS detection, remote access detection, and virtual machine recognition, the suggested advanced features—including structured databases, scheduled scanning, device profiling, intrusion detection system (IDS) capabilities, network forensics, user activity logs, traffic monitoring, and customized report generation—significantly enhance functionality and scope. The integration of blockchain technology introduces immutable logging of security events, decentralized verification of compliance checks, and automated policy enforcement via smart contracts, ensuring a tamper-proof and trustworthy security framework. Specifically, device profiling and user activity logs, now secured on the blockchain, identify deviations from established security configurations and usage patterns, directly addressing policy compliance. This blockchain-enhanced approach streamlines security analysis, improves detection accuracy, and reduces administrative overhead by integrating multiple security tools into a cohesive, reliable solution.

Keywords: blockchain; cybersecurity; network security; automated detection; threat detection; smart contracts; policy compliance; enterprise security; security auditing; digital forensics; network traffic monitoring; advanced threat detection; real-time network monitoring; network traffic analysis; decentralized verification

1. Introduction

In recent years, with the enriched convergence of the latest technologies whereby users can access, share, and store data through diverse devices and networks in real-time, there has been a significant increase in cybersecurity risks. Organizations face a growing challenge in safeguarding their digital assets against a spectrum of evolving threats. Network infrastructures are particularly vulnerable, with attackers having sophisticated techniques such as rogue access points and man-in-the-middle attacks to compromise Wi-Fi networks and steal user credentials. Attackers can successfully impersonate corporate access to steal user credentials, like, , usernames and passwords, by setting up rogue APs. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks remain a persistent threat, disrupting network availability by overwhelming target systems with malicious traffic [1].

Enterprise systems can experience severe security threats in case the vulnerabilities are left unnoticed, thereby leaving significant exposure of data to the attackers. For enterprises, this can result in prolonged downtime of the systems, which can cause a huge loss of productivity and revenue. The absence of appropriate security measures and particular controls in place to protect sensitive data can lead to an attack. Certain attacks are passive and include observing and data-stealing, whereas active

 doi:10.20944/preprints202505.1028.v1

attacks are intended to destroy or corrupt the data and the network infrastructure. Therefore, if the proper security measures are not in place, then the data and networks are vulnerable to any of these attacks [2]. The organizations take appropriate measures and install different software to protect their data and systems from different attacks. These security measures do not protect the organizations completely, as every day new attacks are introduced and vulnerabilities are found in security software; hence, this software is required to be patched on time. Any business that is seriously concerned about security can particularly focus on patch management, enhanced cybersecurity measures within the organization, and the possibility of considering cyber insurance to transfer residual risk in case of a cyber attack [3]. A critical vulnerability lies in unpatched software, which can expose enterprise systems to severe security breaches, data breaches, and financial losses. Effective patch management is therefore paramount, yet it presents significant challenges due to the rapid discovery of new vulnerabilities and the complexity of maintaining up-to-date systems [4]. It is observed that security breaches in an enterprise network are mostly caused by the absence of updated patches in an enterprise's operating system (OS) along with other applications. For instance, it requires a large amount of commitment and time to update all of the systems whenever a patch update is available in the IT department [5]. Moreover, the rise of advanced threat actors, who leverage artificial intelligence and machine learning to automate attacks and evade traditional security measures, necessitates a multi-layered security approach [6].

For organizations that have digital infrastructures in place, network security is an essential consideration in coping with certain potential cyberattacks. As it is very difficult to completely secure the organization's network just by installing the software, the organizations also take some other appropriate precautionary measures to ensure the network's security. For this purpose, an organization can make and implement policies to guide and instruct its employees to secure its systems and data. Policies and procedures of any organization must be instigated in conformance with the enterprise's culture and internal practices. This assists in the rapid implementation and adoption of procedures interrelated to the current security standards. James et al., as cited by Taylor [7], state that "The essence of information security is all about people, processes, and controls: the heart of successful security is not pure technology, but a team of well-trained employees who are prepared to use technology as a tool to implement and manage effective IT controls." [8].

Beyond technical controls, organizations must foster a robust security culture through comprehensive policies and employee training. Security policies should be tailored to the organization's unique requirements and aligned with industry best practices, such as those outlined in the NIST Cybersecurity Framework [9]. Some precautions must be taken in the form of a policy to secure the system from intruders and getting hacked. The fundamental elements of an organization's security policy can be about the status of the firewall as enabled and the remote access is disabled. To avoid attackers entering the system through a backdoor, it is necessary to monitor all ports when the system is connected to the Internet. The screenshot of Zenmap [10] (MS Windows version of Nmap) shown in Figure 1 lists all the open ports on a system connected to the Internet. There is a port 137, which is filtered, and the rest of the listed ports have an open state. Services running on all of the listed ports are populated against each port with version information.

 doi:10.20944/preprints202505.1028.v1


```
Nmap scan report for HP-514WH (192.168.10.7)
Host is up (0.00s latency).
Not shown: 65522 closed ports
PORT      STATE    SERVICE         VERSION
135/tcp   open     msrpc           Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
902/tcp   open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp  open     unknown
49664/tcp open     msrpc           Microsoft Windows RPC
49665/tcp open     msrpc           Microsoft Windows RPC
49666/tcp open     msrpc           Microsoft Windows RPC
49667/tcp open     msrpc           Microsoft Windows RPC
49668/tcp open     msrpc           Microsoft Windows RPC
```

Figure 1. Zenmap: Open Ports with Services Information.

Organizational security policies can be enforced through various mechanisms, ranging from simple employee notifications to more sophisticated automated systems. Traditionally, policies were disseminated through manual instructions, but modern approaches emphasize automated enforcement. For instance, endpoint detection and response (EDR) agents can be deployed on network systems to monitor user activity and identify policy violations in real-time [11]. Operating system (OS) hardening is another enforcement method, though it must be balanced against user productivity [12]. The hardening of the Operating System (OS) can be another option to enforce the policy but it will also restrict the users to perform some of their management tasks. Davide et al. tried to enforce a network security policy through software-defined networking (SDN) in an organization [13]. However, it requires a change to shift the whole network to SDN by switching all network devices.

A reliable method to audit and evaluate an organization's policies is a network scanner as most of the scanners of network scanners already can check different security aspects like firewall status, shared directories, server recognition, OS detection, remote access detection, and virtual machine recognition in one way or another. We propose an advanced network scanner linked with a structured database that enables us to scan assets and asset groups, view vulnerable assets and their complete security information, schedule scans, e-mail scan reports, and take appropriate action to safeguard our assets based on the remediation solutions provided. It can help to recognize available network devices, and services, identify any filtering systems in place and operating Systems (OSs) in use, and discover vulnerabilities to protect the network from potential attacks. Since security is a major concern for organizations, network scanning enables a security analyst to detect devices present over the network that could be more likely to be exploited by hackers. We also proposed some advanced features in the scanner with which its capability can be greatly improved. These features are network forensics, device profiling, user activity monitoring, IDS capability, and report generation of multiple types.

Blockchain technology, known for its decentralized and immutable ledger, offers a transformative approach to enhancing network security and policy compliance in digital enterprises. By integrating blockchain into network security systems, organizations can ensure that logs of network activities and policy violations are tamper-proof, providing a reliable audit trail for forensic analysis and compliance verification. Furthermore, blockchain's smart contracts enable automated enforcement of security policies, triggering predefined actions—such as alerts or device isolation—when violations are detected. This reduces human error, enhances trust in the system, and aligns with the need for a multi-layered security strategy to combat evolving cyber threats.

The rest of the paper is organized as follows: Section II of the paper discusses different network vulnerabilities, attacks on the network, and policy enforcement methods. Section III describes the basic features of a network scanner, and Section IV designates security aspects that can be discovered via a network scanner. The advanced features of the proposed network scanner to enforce security policy are explained in Section V. Section VI provides an overview of Blockchain Implementation Details, and finally, Section VII concludes the paper with some future work.

 doi:10.20944/preprints202505.1028.v1

2. Network Vulnerabilities, Attacks, and Policy Enforcement Methods

An enterprise network may have various weaknesses that can cause different attacks to disrupt organizational services or steal sensitive information. To avoid such kinds of threats, enterprises define their procedures and policies to reduce vulnerabilities. The implementation of these procedures is an administrative job that can be accomplished using different mechanisms. In this section, various network vulnerabilities, policy enforcement methods, and common attacks are discussed.

2.1. Common Network Vulnerabilities

All operating systems (OS) have built-in certain essential security measures that guard against various vulnerabilities, however, any change in the configurations to meet user requirements can make the OS vulnerable without being noticed by the organization. Figure 2 highlight several common vulnerabilities that can be easily exploited by the attackers like, open ports, remote access, shared directories, and disabled firewalls. The following is a brief description of some of these common vulnerabilities.

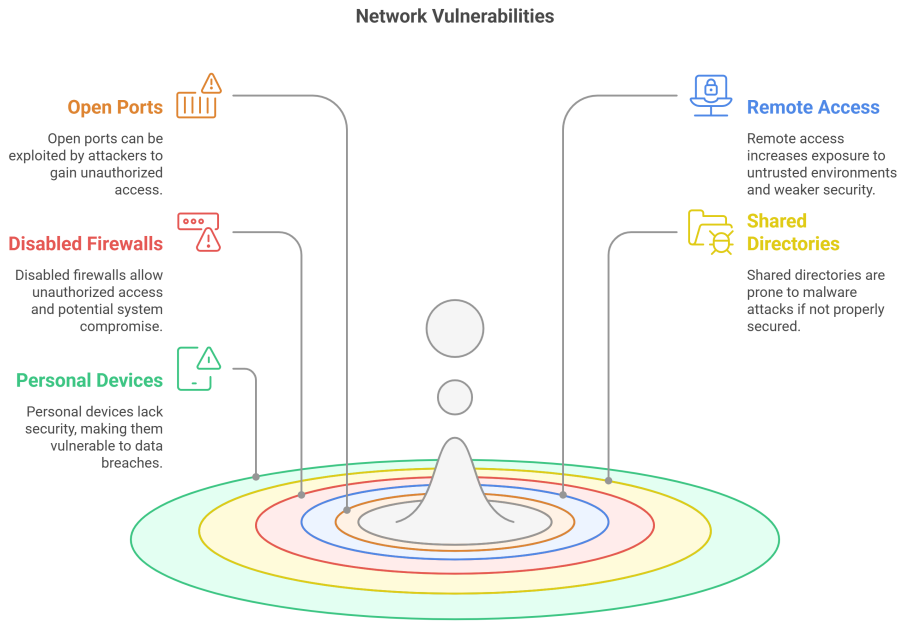

Figure 2. Illustration of Common Network Vulnerabilities Including Open Ports, Remote Access, Disabled Firewalls, and Shared Directories in Enterprise Networks.

2.1.1. Open Ports

In computer networks, an open port is a communication endpoint for accepting incoming connections, usually used by the server applications to cope with requests from remote hosts or clients. Nevertheless, open ports can also accept connections by malevolent clients if these are not protected carefully by exposing prospective weaknesses in the server-side software to remote exploitation. Such an intrinsic vulnerability has always escorted the practice of open ports throughout the account of network services, thus, opening the doors for huge numbers of severe network attacks including TCP SYN flooding attacks. [14]. Smartphone OS also inherits the support of open ports, and since smart devices are significantly dissimilar from the traditional server machines' availability and performance guarantees, therefore, limited information is available about how smart device applications utilize open ports and what the security consequences accordingly [15].

 doi:10.20944/preprints202505.1028.v1

2.1.2. Remote Access

Remote access can be defined as the ability of an enterprise's users to access its office's computing resources from different locations other than the organization's premises. This provision of accessing resources remotely is increasingly common due to the widespread accessibility of smart devices and Internet access. An extensive selection of client hosts across the organization along with several hosts outside the enterprise's control are also reachable through remote access and these hosts usually have weaker safety measures e.g., physical security controls, no corporate-level antivirus tools and firewalls in place. as compared to the systems of an Enterprise. Similarly, organizations do not manage several devices and mostly remote communications are done over untrusted channels. It is quite possible that the remote devices of the client may be used in hostile environments that may not be configured appropriately.

2.1.3. Disabled Firewall

Presently, the protection of data and sensitive information has become a major challenge. Nearly, all the private and public institution's secured data is connected to the internet for diverse purposes. The attackers have many more occasions for getting access to this sensitive information through the Internet. Attacking against a particular network and digital infrastructure is comparatively easy since any network can be accessed from anywhere in the world via the Internet. Therefore, a firewall is an essential and integral part of the organization for protecting systems [16]. Firewall blocks unauthorized attempts to gain control or crash the systems. However, if the firewall is disabled then these systems become vulnerable which can result in numerous unmanaged exceptions. Additionally, this scenario is particularly favorable for the attackers to scan the entire system and may set backdoors without being noticed by the system user which can result in system compromise.

2.1.4. Shared Directories

Over the enterprise network, there can be a commonplace in the digital infrastructure where most of the common resources are shared within the organization. These resources can be accessed by different employees as and when required. Such shared directories can be vulnerable to various cyber threats because a shared directory is accessible over the network therefore, any malware could be placed which can compromise the system and thus overall network. In order to prevent such attacks, it is essential for an organization to keep an eye on shared directories over the network and make them accessible to authorized users only. Advanced IP scanner [17] has the ability to detect shared folders.

2.1.5. Personal Devices

Personal devices such as smartphones, tablets, iPADs, laptops. while connected to organizational networks are vulnerable to various cyber-attacks as these devices usually lack proper security software for their protection. These devices can have viruses or worms and can copy or transfer data against an organization's policy. Bringing personal devices to the organization is the death of perimeter security provided by the organization's border firewall.

2.2. Common Attacks via Network

Attackers gained sufficient skills over the years to find system vulnerabilities, and also utilize advanced intrusion mechanisms that are hard to identify and trace. Network security tools are not only suitable for recognizing security violations successfully but also useful in monitoring attempts to disrupt security [18]. Figure 3 shows that networks are becoming even more vulnerable to a broader variety of security threats. One of the major network requirements is to have several internet access points for private and public networks, therefore, it is essential to secure these networks. Some common attacks on networks are discussed below.

 doi:10.20944/preprints202505.1028.v1

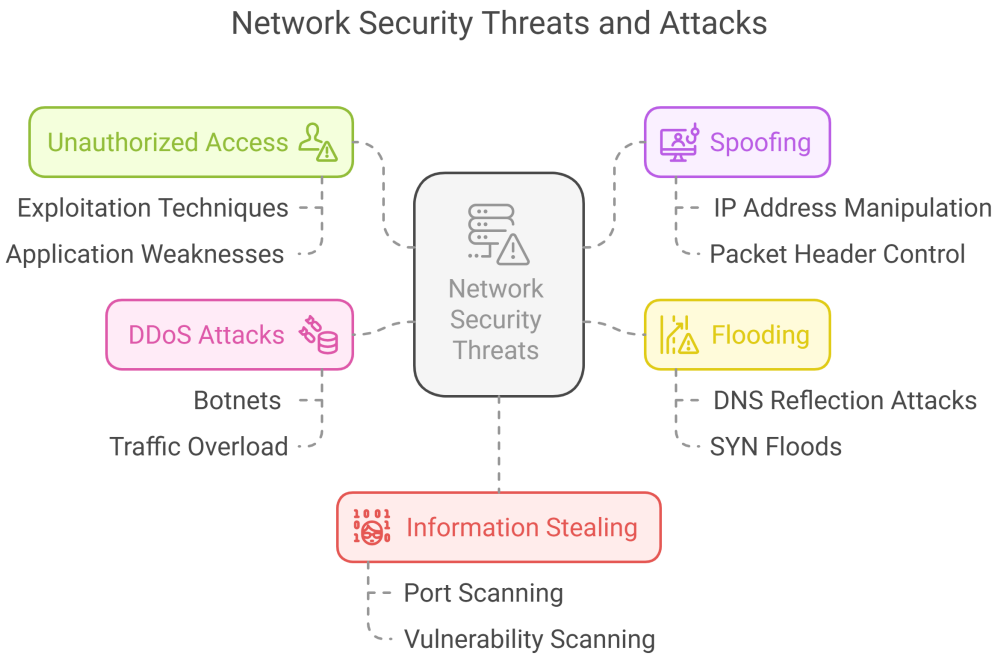

Figure 3. Diagram of Common Network Security Threats and Attacks Such as Unauthorized Access, Spoofing, Flooding, and DDoS in Cybersecurity.

2.2.1. Unauthorized Access

Unauthorized access attacks are intended to provide an attacker with safe access to targeted systems without permission. These attacks usually gain the advantage of the existing vulnerabilities in a targeted system by using well-known exploitation techniques like, scripts or hacking tools, against the targeted system. This contains unauthorized reading, copying, writing, deleting, or sharing information that usually is not available to an attacker. System access is generally extended by making use of identified application weaknesses that could offer partial or full access to a specific system. Likewise, access to a system can be acquired through back doors set up by an attacker or poor application structure during prior system setup [19].

Blockchain can mitigate unauthorized access by implementing decentralized identity management, where user credentials are verified across multiple nodes, reducing reliance on a single point of failure and enhancing access control integrity [20].

2.2.2. Spoofing

IP spoofing happens when the malevolent program generates its packets and does not mention the actual source IP address within the headers of such packets. It is not very difficult to produce individual packets with thorough control in the header of IP and transmit via the same network if one gains sufficient rights in the OS [21]. The intruder captures the IP address of the source system and places this IP address on the packet headers that are being transmitted toward the destination system, thereby evolving the destination machine by ensuring it is an authentic source machine for the attacker that transmits the packets on-demand [8] [22].

By leveraging blockchain for secure data sharing and verification of packet origins, the risk of spoofing can be reduced. Immutable records of legitimate IP addresses stored on the blockchain can help distinguish authentic traffic from spoofed packets.

2.2.3. Flooding

Generally, malevolent software events are furtive, and hence recognition of such actions is a challenging task. An initiating relation can be supposed to be causal and to develop a time-based

 doi:10.20944/preprints202505.1028.v1

affiliation between such events, e.g., in the scenario of a spoofed DDOS flooding attack, the intruder handles a three-way handshake process. During such an attack, the total number of spoofed IP addresses and the open ports utilized by the intruder undergo a causal relationship. DNS reflection attacks and TCP SYN floods are common examples of flooding. Currently, most of the DNS reflection attacks are instigated by spoofing the source IP address to overflow the Internet. For example, SYN floods are spoofed TCP floods, where the source of IP packets looks to be different from their concrete origin. In case the servers are compromised, they can also transfer spoofed packets to generate a large attack. According to Verisign [23], in the second-to-last quarter of the year 2016, there was an enormous strength TCP-SYN flood attack comprising 60 Gigabytes (GB) per second with 150 million packets per second. It was quite a bigger attack than the earlier biggest attack with 125 million packets per second during the last quarter of 2015 [24].

2.2.4. Distributed Denial of Service (DDoS) Attack

The primary objective of DDoS attacks is to deny authentic users' access to different resources of the enterprise network. In Figure 4, an intruder launches a DDoS attack using some zombies and handlers, thereby creating a botnet.

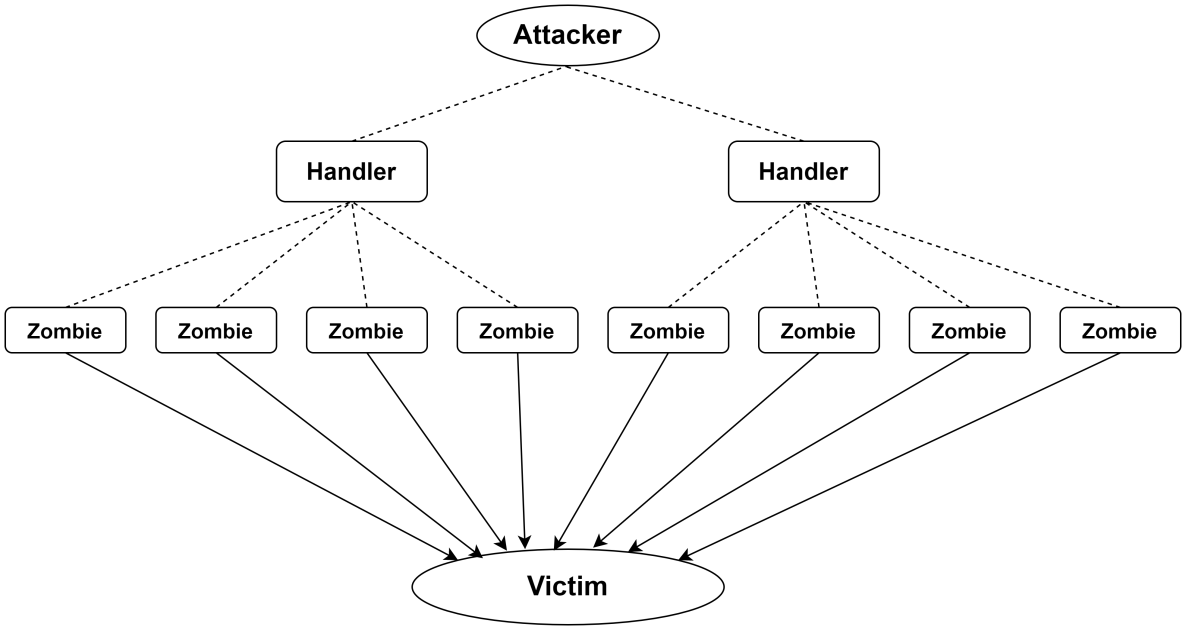

Figure 4. Visual Representation of a Distributed Denial of Service (DDoS) Attack Using Zombies and Handlers to Create a Botnet for Network Disruption.

A botnet may contain hundreds of compromised sources that create capacious traffic to overwhelm the victim. It is tremendously hard to distinguish genuine traffic from attack traffic. It is quite possible that such sources may be spread all around the world [25–28]. Earlier, the DDoS attacks were launched in four (4) different phases like, trade-off, scanning, deployment, and finally propagation. Steadily over the subsequent years, automation mechanisms have been introduced in each of these phases, yet these phases are similar [24].

1. The intruder gathers information about network configuration through port scanners to recognize existing weaknesses in the network.
2. The intruder exploits such vulnerabilities to launch the attack over the organization's network.
3. In case of a successful attempt of attack, the attacker further installs and sets up additional software to manage uninterrupted network access channels.
4. Finally, the intruder struggles to wash-out any remaining evidence that may be left due to the earlier actions. At this stage, daemons restarted that crashed during the 2nd phase, logs were deleted and various actions were taken accordingly.

 doi:10.20944/preprints202505.1028.v1

2.2.5. Information Stealing

Information gathering about a particular network can be done through network port scanning and vulnerability scanning, however, if this job is done by anonymous persons, these are observed as the start of an attack. In scanning processes like, ping sweeps and port scans, explicit information about particular IP addresses mapped to active hosts and the services they provide, is returned. Similarly, the inverse mapping method collects information about IP addresses that do not map to active hosts and this assists the attacker in emphasizing possible IP addresses. During the footprint phase, the attacker creates a profile of the targeted organization including data such as e-mail servers and the domain name system (DNS) of the organization along with its IP address range. In the scanning phase, the attacker determines details about the listed IP address range which can be accessed online, system architecture, OS information, and the list of services running on each system [29]. However, in the enumeration stage, the attacker gathers data like, routing tables, group names, network users, data of Simple Network Management Protocol (SNMP), and so on [5].

Immutable logging on the blockchain ensures that any attempt to steal information is recorded in a tamper-proof manner, aiding in detection and traceability during forensic investigations [30].

2.3. Policy Enforcement Methods

Organizations define their own procedures in the form of policies to safeguard their data and networks and such policies can be implemented in numerous ways from simple instructions to employees to system hardening or installing of monitoring agents in the individual's machines. Some of the common policy implementation mechanisms are discussed in the following subsections:

2.3.1. Guidelines

Organizations must define and document certain security policies in the form of guidelines. These guidelines can be communicated to the employees through various means like, verbally, through email and organizational documents. The next step is to ensure that all of the designed guidelines are implemented and properly followed by the employees. As in this method, there are no checks and balances so the organizations have to trust their employees that they will not violate the policy which seems impossible.

2.3.2. OS Hardening

It is a method of increasing the security of network infrastructure and an OS to improve effective security. The security of an OS can be reinforced by setting up appropriate configurations, eliminating vulnerable services, updating software, and applying security policies e.g., monitoring user logins and enhancing password strength. A comprehensive set of minimum requirements for OS hardening is proposed based on NIST, FIPS, CC. cybersecurity standards [12]. The complexity of OS hardening is influenced by enterprise policies and the skills of the network administrator [31]. The most common exercise is to follow predefined security guidelines that are executed from time to time to ensure that security procedures are in place. The guidelines list can be executed through various auditing tools like, Nmap, Nessus, Open Vulnerability Assessment Scanner (OpenVAS) [32]. This policy enforcement method fails when an employee requests admin privileges to perform certain tasks such as installing specific software, or modifying system configurations. Likewise, if a hypervisor like, VirtualBox or VMWare, etc. is installed, then the employee has a fully flagged OS under his/her control with admin privileges, and the activities performed on this virtual machine will not be detected by the organization.

2.3.3. Agent-Based Enforcement

An agent-based solution to be installed on the host to monitor and to keep track of activities like software installations, file downloads, and, logs. This solution helps to monitor the user activities and manage logs that can be used for further analysis. In this method, the organizations install an agent on

 doi:10.20944/preprints202505.1028.v1

each system of their network, which will inform the server about any violation done by the user but this method can also be bypassed by the employees by disabling the agent.

2.3.4. Restriction Through Software Defined Networking

A modern way to enforce network security policy in an organization is by using software-defined networking (SDN) [13]. Nevertheless, this requires a major transformation by shifting the complete network infrastructure to SDN by replacing all the traditional network devices with OpenFlow-enabled devices.

A trustworthy method to review and enforce an enterprise's procedures is a network scanner that is capable of identifying common vulnerabilities such as a disabled firewall, enabled remote access, virtual machines shared directories. There is a need to develop an advanced network scanner that allows us to scan network assets from time to time, inquire about vulnerable assets and all security information, e-mail scans, and take suitable action to protect assets based on the indemnification solutions provided. As the scanner is an essential tool for a network administrator as well as a penetration tester for the diagnosis and investigation of the enterprise network.

2.3.5. Blockchain-Based Policy Enforcement

Blockchain technology introduces a novel method for policy enforcement by utilizing its decentralized and immutable properties. Security events, such as policy violations detected by the network scanner, can be logged on a blockchain, ensuring they cannot be altered or deleted [33,34]. Smart contracts—self-executing agreements coded on the blockchain—can automate responses to violations, such as isolating a non-compliant device or notifying administrators, without manual intervention. Additionally, a decentralized network of nodes can verify compliance checks, reducing the risk of manipulation and enhancing trust in the enforcement process. This approach complements traditional methods by providing a robust, automated, and auditable framework for policy adherence [35].

3. Basic Features of a Network Scanner

Network scanner offers analysis and assessment for different weaknesses of network systems thereby attaining preemptive protection. It enables the network administrator to recognize some unsafe backdoors, vulnerabilities and overcome such weaknesses before the system is broken. Many of the scanning solutions are generally based on packet capturing and packet crafting libraries like, Libpcap and Libnet.

The proposed network scanner will interface with a blockchain network to store and retrieve critical data, such as scan results and compliance statuses. By recording this information on an immutable ledger, the scanner ensures that security assessments are trustworthy and verifiable, enhancing the reliability of basic features like IP scanning, port scanning, and vulnerability detection.

Libnet [36] library is written by Mike D. Schiffman and can generate and send packets for numerous protocols. Especially, such a system gets a fast and suitable capability that is based on Libnet since it is specifically designed for packet crafting. The procedure of creating network packets is streamlined and packets of each distinct protocol can be generated using Libnet. It offers support for common protocols like, TCP, IP, UDP, ARP, MPLS, RARP, ICMP, and so on [37]. Nmap uses its modified version like, Libdnet, for low-level tasks like sending ethernet frames, etc [38].

Libpcap [39,40] is a generic library designed by Steven McCanne, Craig Leres, and Van Jacobson from the Lawrence Berkeley National Laboratory at the University of California, for packet capturing that offers a high-level interface to packet capture systems. It practices the BPF [41] technique of packet filter to receive the packet rapidly. The original filter expression can be associated with building a much more complex filter expression using "not" "and", and "or". In the Microsoft Windows platform, the Winpcap utility is based on the Libpcap and uses the NPF [42] mechanism. The network scanning and monitoring tool sits within any enterprise network as illustrated in Figure 5. Network scanning comprises some of the core features like port scanning and vulnerability scanning.

 doi:10.20944/preprints202505.1028.v1

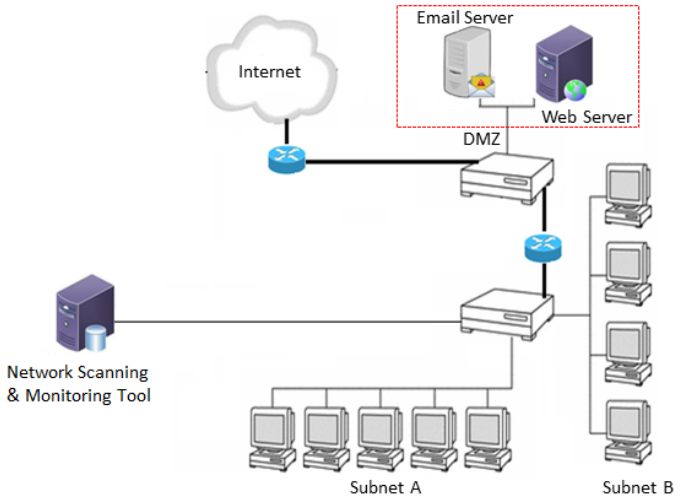

Figure 5. Deployment Architecture of Network Scanning and Monitoring Tools in Enterprise Networks for Enhanced Security and Compliance.

There are several network, IP, Port, and vulnerability scanning tools widely used for security auditing and network scanning. Some of the widely available scanning tools are Nmap [43–45], SolarWinds Port Scanner [46–48], Advanced IP Scanner [17,49] , Angry IP Scanner [50,51], Free IP Scanner by Eusing [52,53], NetCat [54,55], LanSweeper IP Scanner [56–58], MyLanViewer Network/IP Scanner [59–61], Nessus [62–66] and Slitheris Network Discovery [67]. Some of the most common services these scanners provide are discussed below:

3.1. IP Scan

IP scan is a general scan and is the continuing IT job of investigating an enterprise network to determine IP addresses and discover appropriate information related to these IP addresses. It is useful in finding hidden devices (which do not appear in general searches from operating systems) and discovering new devices over the network. Almost all of the aforementioned widely used scanning tools like, Nmap, SolarWinds port scanner. provide IP scanning features to discover the up hosts on the network.

3.2. Port Scan

In port scanning, data packets are sent over the network to the specified service port numbers (e.g., port number 23 for Telnet, and port number 80 for HTTP.) of a targeted system. The goal of port scanning is to discover open ports of the host and get information about the services running on these ports. It is really valuable to get further details from the remote host since ports are opened by different servers like Email servers, FTP servers, Web servers, and so on. TCP and UDP protocols require ports to communicate through the Internet, and every port is a number that identifies different types of service. The port numbers initiated at 1 up to a total of 65535 ports including port numbers of lower ranges are used for general Internet protocols. Through the port scanning method, it can be identified which ports are open, closed, or filtered of any remote host(s). Nmap, SolarWinds with many other scanners have port-scanning features. Generally, port scanning comprises three types: open, half-open, and stealth scan as briefly described below:

3.2.1. Open Scan

An open scan is a process of discovering open ports in a remote host and is mostly done by the network administrator and pen-testers during the analysis of networks using a TCP connection to the destination host. Such types of scans are certainly recognized by the firewalls and usually complete the three-way handshake port scan process [68] [69].

 doi:10.20944/preprints202505.1028.v1

3.2.2. Half-Open Scan

It determines if a port is open by executing the first step of a three-way handshake. The aggressor struggles to set up a TCP/IP connection with a server at each potential port and this is carried out by sending a synchronization (SYN) packet to each port of the server.

3.2.3. Stealth Scan

In this type of port scan, a firewall, filter, or router is bypassed, thereby acting as spontaneous network traffic. Various stealth port scan mechanisms are practiced including NULL scan, FIN scan, and XMUS scan [70].

3.3. Banner Grabbing/OS Detection

In network environments, the system vulnerability is associated with the OS and various OS have their security features. Therefore, before inquiring about the security status of the system the information about the OS must also be understood. In network scanning, the identification of OS should be the first step in network security scanning, can discover suitable information about OS like, OS version, classification., and is also very useful for the discovery of OS vulnerabilities. Since distinct OSs have different kernels and implementation styles thereby the OS detection of a remote host becomes integral to acquiring precise mechanisms to discover the OS vulnerabilities [37]. Banner grabbing can be done through Nmap, Zenmap, Nessues. scanning tools. Nmap stresses identifying the accurate OS of a remote host, however, this may not be possible for every host. In such a case, it labels the percentage with the detected OS. Likewise, SolarWinds Port Scanner offers hostname resolution with particular DNS details and in addition to this, it can also discover MAC addresses to extract the OS and its related information.

3.4. Server Recognition

While scanning the remote host, may require verifying whether the remote host is either a server or a client. This can be achieved by extracting information about some common ports like, 8080, 25. For instance, the port for the SMTP mail server is 25, 21 for FTP and 8080 port number for a web server. The presence of one or more of these open ports on a system represents that the system is working as a server. Nevertheless, none of the major scanning tools provide such features to discover the server machine.

3.5. Vulnerability Scan

Vulnerability discovery is one of the keys to protect computer systems and such weaknesses can be exploited by hackers to get control of the targeted system. The goal of vulnerability scanning is to discover and fix such weaknesses before attackers utilize them against the machine. Various known weaknesses can be identified by the vulnerability scanners and these scanning tools accomplish this objective by following different techniques. The development of a vulnerability scanning tool is to probe a list of supplied ports of a host and attempts to discover the service running at every port for various known vulnerabilities thereby leading to potential threats to the system [37]. However, in vulnerability scanning, the intention is to identify well-known systems vulnerabilities that are present over the network. It facilitates the discovery of particular weaker spots in an Operating System (OS) and the application software, that can compromise or crash the targeted system [71].

Nessus [66] is one of the well-known tools for vulnerability assessment and is a multithreaded-based tool. The vulnerability data supplied by this tool is compatible with Common Vulnerabilities and Exposures (CVE) [72,73] which is a publically available famous dictionary for information security. CVE's general identifiers allow data exchange among security products and offer a baseline index for assessing coverage of tools and services. The management of the CVE dictionary is done by the MITRE Corporation, which generates the list of standardized names for well-known security vulnerabilities and exposures. It is straightforward and facilitates the provision of separate databases to exchange vulnerability data. The vulnerability of the targeted system can be swiftly revised by the

 doi:10.20944/preprints202505.1028.v1

CVE-compatible database in case the information includes a CVE token [19]. Likewise, Nmap provides vulnerability scripts, namely Vulscan and Vulners, which enable network administrators to discover related CVE information from the specific local host machines or remote hosts. Vulscan queries CVE from its local databases that are hosted on the machine containing the Nmap client application. The overall vulnerability scan process can be seen in Figure 6.

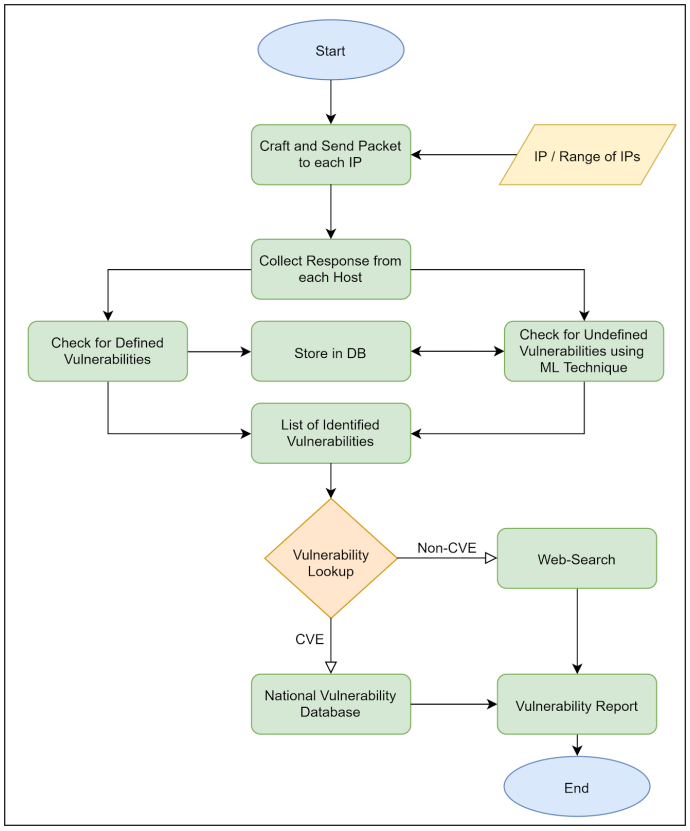

Figure 6. Process Flow of a Vulnerability Scan Identifying Weaknesses in Network Systems and Applications for Cybersecurity Risk Mitigation.

4. Security Aspects Discoverable via Scanner

An attacker discovers the weaknesses using common network and vulnerability scanners before intruding into the system and reveals the security vulnerabilities that compromise the data or steal sensitive information by intrusions. The scanner can verify the integrity of the blockchain ledger used to store security data, ensuring that logs and compliance records remain untampered. It can also monitor the proper execution of smart contracts, confirming that automated policy enforcement actions are triggered correctly. These checks enhance the overall security posture by ensuring the blockchain component operates as intended. A brief overview of some of the common security traits discoverable through a common scanner is given below:

4.1. Firewall Status

A firewall is a perimeter security system installed in a host or network that monitors, controls, and tracks the incoming network traffic, as well as outgoing traffic based on a predefined set of security, controls [74]. It usually generates a blockade between a secure, trusted internal network and an alternative outside network like, the Internet, which is not supposed to be a trusted or secure network. Firewalls are generally categorized into two types like, host-based firewalls and network firewalls. A host-based firewall can be installed and run on a network-connected device or a personal computer and monitor network traffic on that machine. However, the network firewall is a software appliance that can run on a general-purpose hardware-based or hardware firewall system appliances that filter network traffic among two or more networks [16].

 doi:10.20944/preprints202505.1028.v1

Scanners can easily check the status of the firewall on a system via port scanning. For example, Nmap can test and verify the firewall rules and filters while port scanning. It can be verified by simply checking whether the port is open, closed, or filtered. A filtered port means that Nmap is unable to check the status of ports due to firewalls. The TCP ACK scan of Nmap will establish whether network packets can pass through the enterprise firewall unfiltered.

4.2. Remote Access Status

The remote access status of a host can be investigated through a scanner. There are many services that provide remote access such as Windows' RDP, Linux's VNC, Cisco Anyconnect, Teamviewer, and pcAnywhere. The remote access can be verified by examining the corresponding port number for different services such as 3389 for RDP, 5900 for VNC, 1723 for Point-to-Point Tunneling Protocol (PPTP), 5938 for Teamviewer, and 5631-2 for pcAnywhere. To keep the system and data secure, it is essential to make sure that remote access is disabled so that the system can not be accessed remotely. In addition to that network administrators should know that these services may run on any of the available ports, however, the above-mentioned are the default ports for corresponding services.

4.3. Shared Directories

Over the enterprise network, there can be a commonplace in the digital infrastructure where most of the common resources are shared publicly. These resources can be accessed by different employees as and when required. Such a shared directory/file can be vulnerable to various cyber threats, so needs to be protected with some kind of scanning tools. Aside from centralized shared resources, individual employees should not be allowed to share the documents on their systems. To prevent certain threats, it is essential to identify the directories/files shared by the employees on their systems over the network.

4.4. Malicious Services with Open Ports

Services running on the open ports can be easily inquired by the scanner, and information about the services is also available. It is essential to check and verify that there should not be malicious services that are running with the open port(s) of a system.

4.5. Virtual Machines Recognition

A virtual machine has a full OS in control of a system user and can have direct access to the internet so it can have malicious software installed on it with admin privileges. The scanners have the capability of identifying vendor names as well as VM, using the database of vendor lists with defined MAC Address ranges assigned to each vendor. An efficient scanner should identify whether the host is a virtual machine or not.

4.6. IP Conflicts

An IP address is assigned to a system for a specified time period which is renewed when the system maintains the connectivity. If a host is idle for a long time or if a user enables the sleep mode of the system over a longer time, then there may be a possibility that during this time another host joined the network and assigned the same IP address. When the user disables the sleep mode and starts working on the system, there may be chances of duplicate IP addresses. However, another possibility is that a duplicate IP address to be assigned from an unauthorized or 'rogue' DHCP server connected to a subnet. Duplicate IP addresses are usually automatically found by the operating systems during the DHCP address assignment process.

4.7. Wake on LAN

A system can be switched ON remotely by any other system knowing the MAC address over the network. This can only be done if this functionality is enabled on a system. A scanner should verify that the wake on LAN property should be disabled to avoid any potential cyber-attacks.

 doi:10.20944/preprints202505.1028.v1

As discussed in Section II, network security policy enforcement is the key to basic security measures. If the employees of organizations do not follow and apply the security policy on their systems then border firewalls become useless. As malicious software can penetrate the network from personal devices like laptops or cell phones of employees. Therefore, these devices should be monitored regularly. most organization relies on a central protection system and leave the employee systems unchecked, as it is very difficult to check each system individually for policy violations. In the next section, we discuss the advanced features of the proposed scanner.

5. Blockchain Implementation Details

The proposed system employs a permissioned blockchain network, where authorized nodes—such as network scanners and administrative servers—participate in consensus. A Hyperledger Fabric-based architecture is suggested due to its support for private channels and smart contracts (chaincode), ensuring data confidentiality within the enterprise. The blockchain stores hashes of scan results, logs, and compliance records, with full data optionally kept off-chain for efficiency, linked via cryptographic pointers. The details of implementation are visualized in Figure 7.

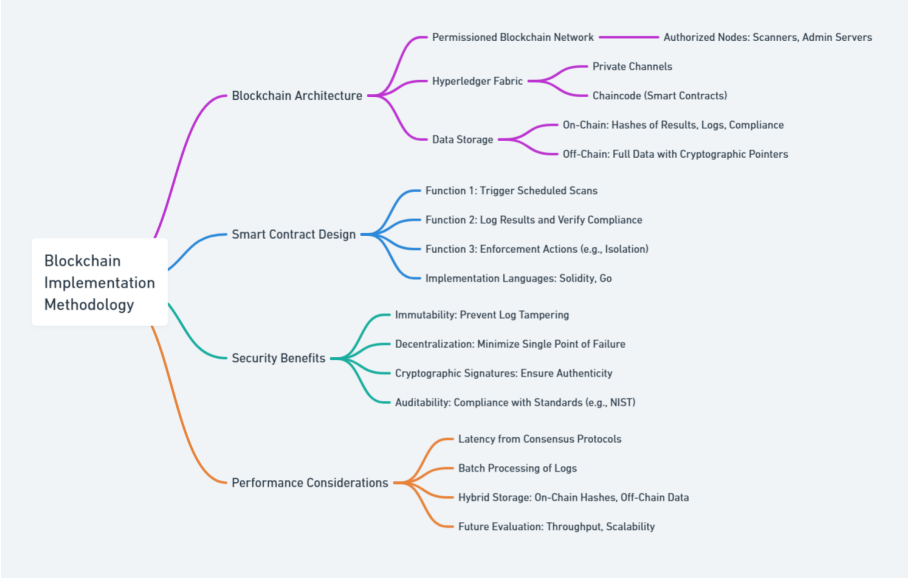

Figure 7. Mind Map Detailing Blockchain Implementation Methodology for Secure and Immutable Network Security Policy Enforcement.

5.1. Smart Contract Design

Smart contracts are implemented to automate key functions: (1) triggering scheduled scans and logging results, (2) verifying device compliance against policy rules, and (3) executing enforcement actions (e.g., device isolation). These contracts are written in a language like Solidity or Go, depending on the platform, and deployed on the blockchain network.

5.2. Security Benefits

The immutability of blockchain prevents log tampering, while decentralization reduces single points of failure. Cryptographic signatures ensure data authenticity, and auditability supports compliance with standards like NIST.

5.3. Performance Considerations

Blockchain integration may introduce latency due to consensus mechanisms. To mitigate this, batch processing of logs and hybrid storage (on-chain hashes, off-chain data) are recommended. Future evaluations will assess throughput and scalability under real-world conditions.

 doi:10.20944/preprints202505.1028.v1

6. Proposed Scanner with Advanced Features

To keep an eye on every aspect related to network security, there is a need to develop a network scanner with more advanced features than the scanners available on the market. The scanner should be able to detect the discovery of new devices automatically as well as the disappearance of existing devices. In addition to that, keeping the device profiles and scanning history for the purpose of network forensics is also necessary. To achieve this functionality, a scanner can be linked to a structured database like SQL, for record-keeping.

By keeping the different security aspects in mind, in light of the previous discussion, we proposed a network scanner with some advanced features like asset profiling, scheduled scans, security policy violation detection, and comprehensive report generation. The proposed network scanner operates through a systematic approach, as described in Algorithm 1. It includes device discovery, traffic monitoring, policy enforcement, and report generation.

Algorithm 1 Proposed Network Scanning and Monitoring Algorithm

```
Initialize: Network Scanner with Database Connection
Input: Network Range, Scan Frequency, Policy Rules
Output: Device List, Traffic Logs, Policy Violation Reports
procedure NetworkScan
    Retrieve stored device profiles from database
    Scan for active devices on the network
    for each detected device do
        if device is new then
            Generate alert and add to database
            Perform DeviceProfiling(device)
        else
            Update last seen timestamp
        end if
    end for
end procedure
procedure DeviceProfiling(device)
    Identify device type (Laptop, Mobile, Printer)
    Retrieve MAC and IP addresses
    Check OS and installed software
    Store profile in database
end procedure
procedure TrafficMonitoring
    Capture and log network traffic (Packet Headers Only)
    for each packet do
        Extract Source and Destination IP, MAC, and Ports
        Log activity in database
    end for
end procedure
procedure PolicyEnforcement
    for each device in network do
        if Policy Violation Detected then
            Generate alert and log violation
        end if
    end for
end procedure
procedure GenerateReports
    Retrieve stored logs from database
    Compile network status, violations, and device profiles
    Export report in PDF format
end procedure
```

 doi:10.20944/preprints202505.1028.v1

The scanner with advanced features can help administrators check policy violations and other security issues. The proposed scanner with major advanced features can be seen in Figure 8 and is briefly discussed below:

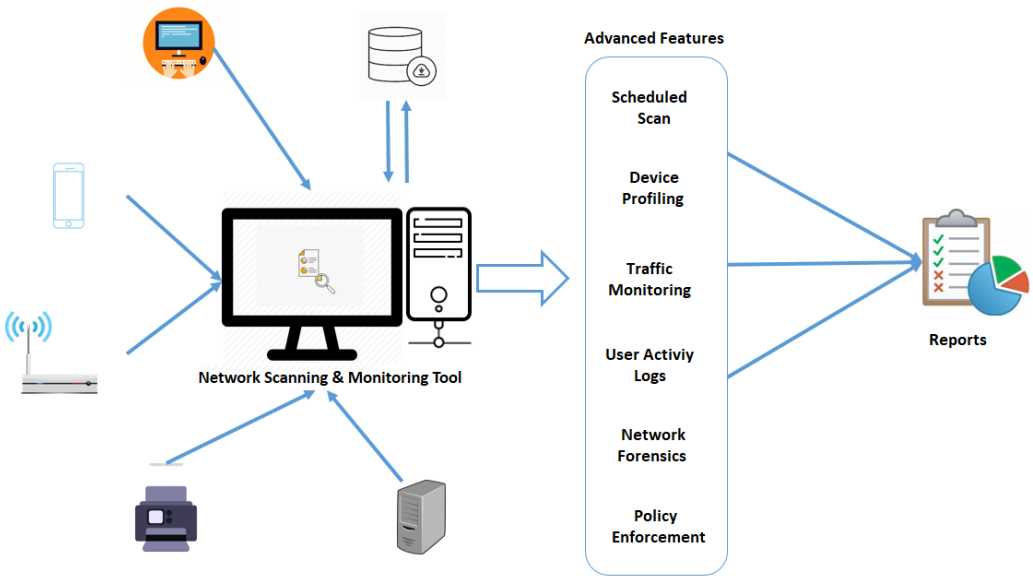

Figure 8. Architecture of the Proposed Advanced Network Scanning and Monitoring Tool with Blockchain Integration for Automated Policy Violation Detection.

6.1. Local Database

The traditional scanner does not have a structured database to store the scanning results, therefore, the results of the previous scans not be retrieved or queried if required. So, to link a scanner with a structured database is the first step toward the advanced scanner and will be very useful in order to associate current results with previous scans. Furthermore, the linked database can store and provide the complete connection history of a specific device with associated IP addresses and timestamps.

Instead of relying solely on a traditional structured database like SQL, the proposed scanner integrates a blockchain-based database to store scan results, device profiles, and activity logs. This ensures data immutability and transparency, allowing multiple stakeholders to verify records without the risk of tampering. The blockchain complements the local database by providing a decentralized, secure storage layer for critical security information.

6.2. Scheduled Scanning

A scheduled scan is a network audit that is scheduled to run automatically on a specific date/time and at a specific frequency. A network scanner should have this feature in order to scan the network automatically. Scheduled scans can be set to execute once a day or periodically with different parameters. Scanning during working hours can help in monitoring and tracking of connected devices. Scanning results can be stored in a database and maintained accordingly. The major benefit of scheduled scanning is regular inventory checks and employees' activities during working hours. The connection history of connected devices in a network can be stored for future references and event logs of connected devices are maintained regularly.

Scheduled scanning is enhanced by blockchain through the use of smart contracts. These contracts can be programmed to trigger scans at specified intervals, log the results on the blockchain, and automatically initiate remediation actions if policy violations are detected. This automation reduces administrative overhead and ensures consistent monitoring.

 doi:10.20944/preprints202505.1028.v1

6.3. Device Profiling

It is quite useful for enterprises to know about each device connected to its network, especially in situations when there isn't any defined policy by an enterprise about Bringing your own Device (BYOD). Hence, the personal devices of the employees will be directly connected to the enterprise network without any restriction. Therefore, device profiling is very important for an organization in order to know about the attached devices, their types (like laptop, cellphone, tab.), OS installed, first discovery on the network, and the owner's name as well. Device profiling is illustrated in Figure 9. This feature will enable an organization to identify devices. This can help the network administrator to check if any malicious system or disgruntled employee is attached to the network. Thereby, it would assist in preventing any potential attack or theft of information. The addition of any new system (host) or the removal of the existing system can also be tracked through this network inventory.

Device profiles are stored on the blockchain, making them tamper-proof and verifiable across the network. Each profile, including device type, OS, and owner details, is recorded as a blockchain transaction, ensuring an auditable history of device connections and compliance status.

6.4. New Device Discovery

On day-to-day network scanning, it is obvious to maintain and manage the inventory of the overall network devices. The list of newly discovered devices can be extracted from the list of active hosts during the device discovery process, as shown in Figure 9. Therefore, whenever a device is discovered for the first time, a scanner should generate an alert and try to get more and more information about it. This information can be stored in the database after verification and filling in the empty attributes.

When a new device is discovered, its details are added to the blockchain via a transaction. Smart contracts can then automatically verify compliance with organizational policies—such as checking for disabled remote access or enabled firewalls—and flag non-compliant devices for immediate action.

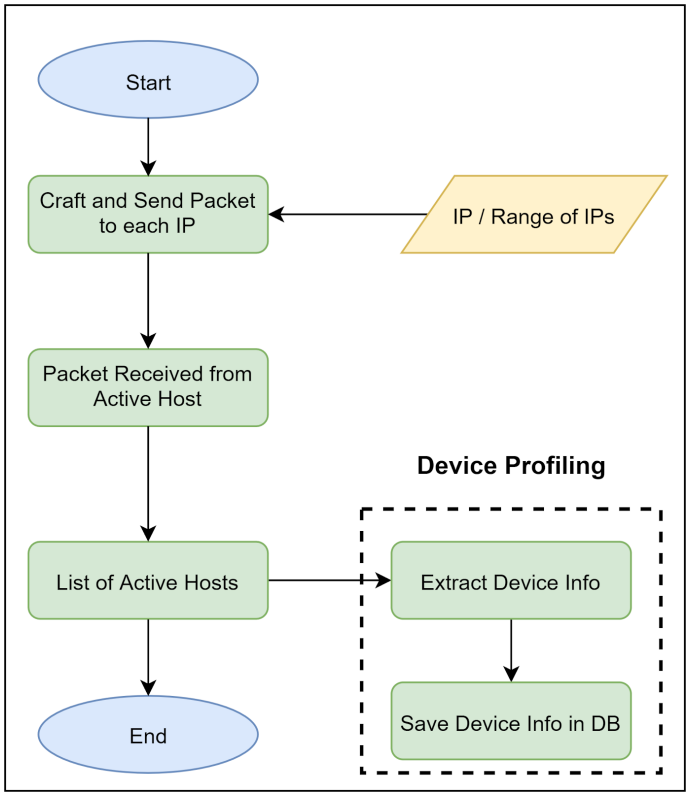

Figure 9. Device Discovery and Profiling Process in Network Security for Identifying and Managing Connected Devices in Enterprise Environments.

 doi:10.20944/preprints202505.1028.v1

6.5. Traffic Monitoring

Although traffic monitoring is out of the scope of a network scanner, it will be very useful if a limited traffic monitoring functionality is added to it as almost all the scanners already have a Libpcap library to decode packets. This purpose can be achieved by connecting the scanner to a switch's mirroring port with a dedicated line to transfer a copy of each packet passing through the network toward the scanner. Only the packet header data is enough for analysis and record purposes and there is no need to inspect the packet payload as it requires heavy processing and machine learning algorithms.

Traffic logs, including packet header data (MAC addresses, IP addresses, and ports), are recorded on the blockchain. This provides an immutable record of network activities, enabling reliable analysis and traceability while preventing log manipulation by malicious actors.

From packet header data we can easily extract the MAC addresses, IP addresses, and port numbers, which can help us to recognize the devices and services they are using. The device monitoring process is illustrated in Figure 10.

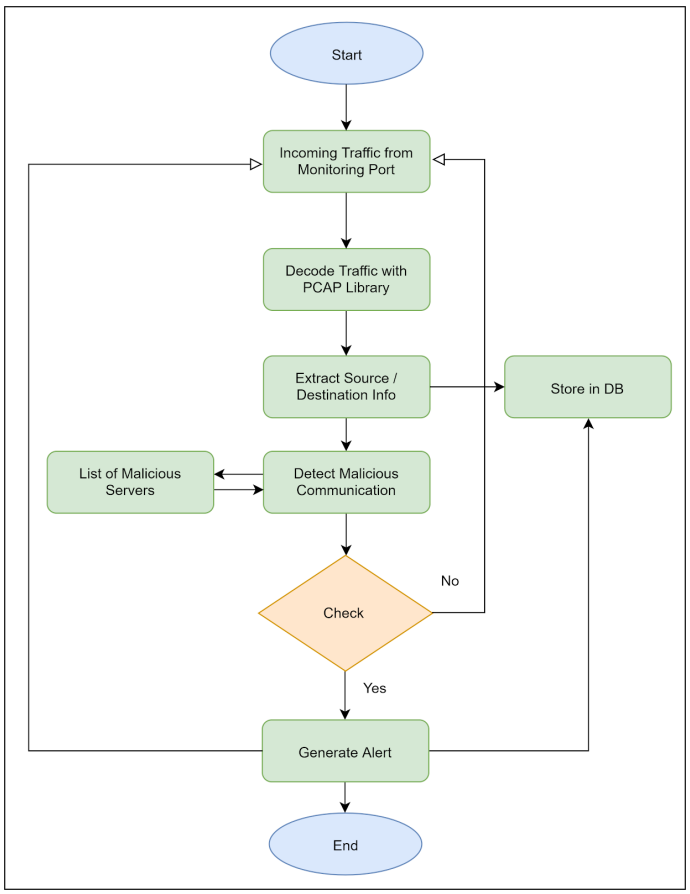

Figure 10. Real-Time Device Monitoring in Network Security Systems for Tracking and Analyzing Network Traffic and User Activity.

6.6. User Activity Logs

The user activity logs are important to know about a user's activeness or idleness on a network in order to evaluate their performance. The limited traffic monitoring feature of a scanner enables an organization to record the employee's activity hours and match it with the attendance management system. Furthermore, this feature can also help to detect any activity after office hours on a system or network.

User activity logs are secured on the blockchain, ensuring that records of employee actions—such as login times or policy violations—cannot be altered. This enhances accountability and supports forensic investigations by providing a tamper-proof activity history.

 doi:10.20944/preprints202505.1028.v1

6.7. Network Forensics

Keeping a record of network activities (like, information about connected devices, service details, user activities, and various events) is getting important day by day. The linking of a database with a network scanner makes it more powerful to collect and store these records regularly. These records can be very helpful and can provide limited help (like, device type, OS info, IP address, services) in the network forensics process in case of any security incident or a cyber-attack. Therefore, network forensics feature availability in the advanced scanner will be quite useful for all kinds of organizations nowadays.

The blockchain's immutable nature makes it ideal for network forensics. Records of device connections, traffic patterns, and security events stored on the blockchain provide a reliable, unalterable evidence base, facilitating detailed analysis following a security incident.

6.8. IDS/IPS Capability Detection

The purpose of the IDS/IPS is the timely identification and prevention of potential attacks from the internet. Nevertheless, the management of IDS/IPS systems may not be affordable for small to medium-sized enterprises. Again, this feature is out of the scope of a network scanner, but most of the scanners have the capability to craft network packets with the support of various libraries. Therefore, a scanner can be used to create spoofed packets to launch a flooding attack against a system in order to assess its capability to detect and prevent attacks. This feature will easily access the resistance of a network asset against flooding, spoofing, and denial of service attacks.

Results of IDS/IPS capability tests are logged on the blockchain, creating a verifiable history of the system's security posture. Smart contracts can analyze these results and trigger alerts or mitigation steps if vulnerabilities are detected, enhancing proactive defense.

6.9. Blockchain Integrity Checks

The scanner can verify the integrity of the blockchain ledger used to store security data, ensuring that logs and compliance records remain untampered. It can also monitor the proper execution of smart contracts, confirming that automated policy enforcement actions are triggered correctly. These checks enhance the overall security posture by ensuring the blockchain component operates as intended.

6.10. Policy Enforcement

As discussed in section II, network security policy enforcement is the key to basic security measures. A scanner can be a very useful tool to check security violations, like, shared remote access, firewall disabling, directory sharing, and connecting a personal device to a secured organizational network. The scanner with the proposed features discussed above will be able to scan the whole network automatically without human involvement and will produce detailed reports in case of any policy violation found on the employee's system.

Blockchain-enabled smart contracts automate policy enforcement by executing predefined actions when violations are detected. For example, if a scanner identifies a disabled firewall, a smart contract can isolate the device and log the event on the blockchain, ensuring rapid response and an auditable record of compliance actions.

6.11. Customized Report Generation

All the aforementioned features of the scanning tool may not be very effective without the generation of comprehensive reports of the various network scans, monitoring activities, irregularities, policy violations, and other issues. An advanced scanning tool must provide comprehensive and multipurpose customized reports that are exportable in various formats, such as PDF, web-based. These reports can be shared with the organization's management and leadership to inform them about any malicious activity in the network, like spoofing, flooding. will be described in the irregularities report. In addition to that, many custom reports can also be generated on a daily, weekly, or monthly basis as per the demands of the organization. For example, a general scan report should be generated

 doi:10.20944/preprints202505.1028.v1

on a daily basis having information about various in-depth scans. Similarly, the policy enforcement reports in case of any non-compliance with the organizational policy detected from any of the devices in the network must be reported on a daily basis.

Reports are generated based on data retrieved from the blockchain, ensuring accuracy and integrity. These blockchain-backed reports—covering scan results, violations, and forensic data—can be shared with management in formats like PDF, providing a trustworthy overview of network security status.

The vulnerability reports can be generated on a weekly basis containing detailed information about each connected device and patchable vulnerabilities found in these devices. The report about the monitoring activities containing information about the host usage and its last active time can be generated every month. The proposed system will get the activity logs from the database saved by the limited traffic monitoring feature as discussed in section 5.6. In case the vulnerability is identified a host should monitor after informing the related person, whether the patches are installed or not. In the latter case, a report can be generated and sent to the organizational management for corresponding actions.

In Table 1 a quantitative comparison of the existing network, port, IP, and vulnerability. Scanners are provided. It comprises thirteen (13) attributes for comparison, including common features offered by the various existing scanning tools and some advanced features that are not offered by these tools.

Table 1. Comparative Analysis Table of Existing Network, IP, Port, and Vulnerability Scanners Highlighting Features Like Firewall Status, Remote Desktop Status, and Policy Enforcement.

Name	FWS	RDS	VMD	UP	DI	CR	VD	NF	IDSE	SS	SD	PE	TM
NMAP	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
SolarWinds Scanner	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗
Advanced IP Scanner	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Angry IP Scanner	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Eusing IP Scanner	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
NetCat	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
LanSweeper IP Scanner	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗
MyLanViewer	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Slitheris Network Discovery	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
Proposed Advanced Scanner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

7. Conclusions and Future Work

Security policies are vital for protecting organizational networks, yet enforcing them at a granular level remains challenging. This paper proposes an advanced network scanner with features like device profiling, scheduled scanning, and traffic monitoring to detect policy violations effectively. The integration of blockchain technology significantly enhances this framework by providing immutable logging, decentralized verification, and automated enforcement via smart contracts. These capabilities ensure tamper-proof records, reduce manual oversight, and improve trust in compliance processes. Compared to traditional methods like OS hardening or SDN-based enforcement, this blockchain-enhanced approach is cost-effective and scalable. In the future, we plan to implement the proposed scanner using a specific blockchain platform, such as Ethereum or Hyperledger, and evaluate its performance in terms of latency, scalability, and security. Additional research could explore advanced cryptographic techniques, like zero-knowledge proofs, to further enhance privacy and efficiency in policy enforcement.

 doi:10.20944/preprints202505.1028.v1

Abbreviations

The following abbreviations are used in this manuscript:

SYN	Synchronize
CR	Custom Reports
UP	User Profiling
CC	Common Criteria
FWS	Firewall Status
OS	Operating System
NF	Network Forensics
IP	Internet Protocol
PE	Policy Enforcement
SS	Scheduled Scanning
DNS	Domain Name System
TM	Traffic Monitoring
SD	Structured Database
IDSE	IDS/IPS Evaluation
VMD	Three letter acronym
RDS	Remote Desktop Status
VD	Vulnerability Detection
UDP	User Datagram Protocol
VMD	Virtual Machine Detection
VMD	Virtual Machine Detection
ARP	Address Resolution Protocol
TCP	Transmission Control Protocol
MPLS	Multiprotocol Label Switching
ICMP	Internet Control Message Protocol
RARP	Reverse Address Resolution Protocol
FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology

References

1. Douligeris, C.; Mitrokotsa, A. DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. *Computer Science Review* **2022**, *44*, 100458.
2. Saleem, B.; Ahmed, M.; Zahra, M.; Hassan, F.; Iqbal, M.A.; Muhammad, Z. A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review* **2024**, *5*, 533–561.
3. Muhammad, Z.; Straub, J. An Analysis of Cyber Threats and the Protective Role of Cyber Insurance in the US Market. In Proceedings of the World Congress in Computer Science, Computer Engineering & Applied Computing. Springer, 2024, pp. 259–272.

 doi:10.20944/preprints202505.1028.v1

4. Dissanayake, N.; Jayatilaka, A.; Zahedi, M.; Babar, M.A. Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology* **2022**, *144*, 106771.
5. Rahman, A.; Kawshik, K.R.; Sourav, A.A.; Gaji, A.A. Advanced Network Scanning. *American Journal of Engineering Research (AJER)* **2016**, *5*, 38–42.
6. Buczak, A.L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 1121–1153.
7. Taylor, R.W.; Fritsch, E.J.; Liederbach, J. *Digital crime and digital terrorism*; Prentice Hall Press, 2014.
8. Zhang, C.; Hu, G.; Chen, G.; Sangaiah, A.K.; Zhang, P.; Yan, X.; Jiang, W. Towards a SDN-based integrated architecture for mitigating IP spoofing attack. *IEEE Access* **2017**, *6*, 22764–22777.
9. of Standards, N.I.; Technology. Framework for Improving Critical Infrastructure Cybersecurity, 2018.
10. Zenmap - Official cross-platform Nmap Security Scanner GUI.
11. Sarker, I.H.; Kayes, A.; Badsha, S.; Alqahtani, H.; Watters, P.; Ng, A. Cybersecurity data science: An overview from machine learning perspective. *Journal of Big data* **2020**, *7*, 1–29.
12. Hamdani, S.W.A.; Abbas, H.; Janjua, A.R.; Shahid, W.B.; Amjad, M.F.; Malik, J.; Murtaza, M.H.; Atiquzzaman, M.; Khan, A.W. Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)* **2021**, *54*, 1–36.
13. Berardi, D.; Callegati, F.; Melis, A.; Prandini, M. Security network policy enforcement through a SDN framework. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, 2018, pp. 1–4.
14. Toyeer-E-Ferdoush.; Rahman, H.; Hasan, M. A convenient way to mitigate DDoS TCP SYN flood attack. *Journal of Discrete Mathematical Sciences and Cryptography* **2022**, *25*, 2069–2077.
15. Jia, Y.J.; Chen, Q.A.; Lin, Y.; Kong, C.; Mao, Z.M. Open doors for bob and mallory: Open port usage in android apps and security implications. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2017, pp. 190–203.
16. Bhakthavatsalam, P.; Malarkodi, B. Analysis of network infrastructure threats using SonicWALL analyser. In Proceedings of the 2016 3rd International Conference on Devices, Circuits and Systems (ICDCS). IEEE, 2016, pp. 6–9.
17. Rahman , A.; Kawshik, K.R.; Sourav, A.A.; Gaji, A.A. Advanced Network Scanning. *American Journal of Engineering Research (AJER)* **2016**, *5*, 38–42.
18. Kumar, S. Classification and detection of computer intrusions. PhD thesis, PhD thesis, Purdue University, 1995.
19. Mohammed, S.A. Designing Rules to Implement Reconnaissance and Unauthorized Access Attacks for Intrusion Detection System. *Iraqi Journal of Information & Communications Technology* **2019**, *2*, 25–43.
20. Shahid, J.Z.; Cimato, S.; Muhammad, Z. A Sharded Blockchain Architecture for Healthcare Data. In Proceedings of the 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2024, pp. 1794–1799.
21. Lichtblau, F.; Streibelt, F.; Krüger, T.; Richter, P.; Feldmann, A. Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses. In Proceedings of the Proceedings of the 2017 Internet Measurement Conference, 2017, pp. 86–99.
22. Singh, R.; Thakur, K.; Singh, G.; Gupta, S. Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network. In Proceedings of the Proceedings of the Third International Conference on Advanced Informatics for Computing Research, 2019, pp. 1–10.
23. Verisign.
24. Deka, R.K.; Bhattacharyya, D.K.; Kalita, J.K. Granger Causality in TCP Flooding Attack. *IJ Network Security* **2019**, *21*, 30–39.
25. Ahmed, A.A.; Zaman, N.A.K. Attack Intention Recognition: A Review. *IJ Network Security* **2017**, *19*, 244–250.
26. Baishya, R.C.; Hoque, N.; Bhattacharyya, D.K. DDoS Attack Detection Using Unique Source IP Deviation. *IJ Network Security* **2017**, *19*, 929–939.
27. Sattar, I.; Shahid, M.; Abbas, Y. A review of techniques to detect and prevent distributed denial of service (DDoS) attack in cloud computing environment. *International Journal of Computer Applications* **2015**, *115*.
28. Sun, J.R.; Hwang, M.S. A New Investigation Approach for Tracing Source IP in DDoS attack from Proxy Server. In Proceedings of the ICS, 2014, pp. 850–857.
29. Jung, J.; et al. Real-time detection of malicious network activity using stochastic models. PhD thesis, Massachusetts Institute of Technology, 2006.

 doi:10.20944/preprints202505.1028.v1

30. Arshad, J.; Talha, M.; Saleem, B.; Shah, Z.; Zaman, H.; Muhammad, Z. A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry. *Blockchains* **2024**, *2*, 195–216.
31. Teodoro, N.; Gonçalves, L.; Serrão, C. NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015, Vol. 1, pp. 418–425.
32. OpenVAS. OpenVAS - Open Vulnerability Assessment Scanner. [Accessed: 2020-06-02].
33. Irfan, M.; Ali, S.T.; Ijlal, H.S.; Muhammad, Z.; Raza, S. Exploring the synergistic effects of blockchain integration with IoT and AI for enhanced transparency and security in global supply chains.
34. Islam, M.B.E.; Haseeb, M.; Batool, H.; Ahtasham, N.; Muhammad, Z. AI threats to politics, elections, and democracy: A blockchain-based deepfake authenticity verification framework. *Blockchains* **2024**, *2*, 458–481.
35. Daidone, F.; Carminati, B.; Ferrari, E. Blockchain-based privacy enforcement in the IoT domain. *IEEE Transactions on Dependable and Secure Computing* **2021**, *19*, 3887–3898.
36. Schiffman, M. The libnet packet construction library. *The Million Packet March* **2005**.
37. Liu, W. Design and implement of common network security scanning system. In Proceedings of the 2009 International Symposium on Intelligent Ubiquitous Computing and Education. IEEE, 2009, pp. 148–151.
38. Calderon, P. *Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips*; Packt Publishing Ltd, 2021.
39. Jacobson, V.; McCanne, S. libpcap: Packet capture library. *Lawrence Berkeley Laboratory, Berkeley, CA* **2009**.
40. Shuguang, W.; Gaogang11, X. libpcap-MT: A General Purpose Packet Capture Library with Multi-Thread. *Journal of Computer Research and Development* **2011**, *5*, 756–764.
41. McCanne, S.; Jacobson, V. The BSD Packet Filter: A New Architecture for User-level Packet Capture. In Proceedings of the USENIX winter, 1993, Vol. 46.
42. Risso, F.; Degioanni, L. An architecture for high performance network analysis. In Proceedings of the Proceedings. Sixth IEEE Symposium on Computers and Communications. IEEE, 2001, pp. 686–693.
43. Nmap: The Network Mapper.
44. Shah, M.; Ahmed, S.; Saeed, K.; Junaid, M.; Khan, H.; et al. Penetration Testing Active Reconnaissance Phase–Optimized Port Scanning With Nmap Tool. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2019, pp. 1–6.
45. Lyon, G. Nmap: The network mapper–Free security scanner. *Nmap. org* **2016**.
46. SolarWinds Network Management Tools.
47. Dutta, N.; Jadav, N.; Dutiya, N.; Joshi, D. Using Honeypots for ICS Threats Evaluation. In *Recent Developments on Industrial Control Systems Resilience*; Springer, 2020; pp. 175–196.
48. Phase, E. Scanning and Enumeration Phase **2019**.
49. Advanced IP Scanner.
50. Angry IP Scanner.
51. Dandan, T. Angry IP Scanner. *Cyber security and information* **2017**, p. 87.
52. Free IP Scanner by Eusing.
53. Baloch, R. *Ethical hacking and penetration testing guide*; CRC Press, 2017.
54. The GNU Netcat.
55. Kurth, M.; Gras, B.; Andriesse, D.; Giuffrida, C.; Bos, H.; Razavi, K. NetCAT: Practical Cache Attacks from the Network, 2020.
56. LanSweeper IP Scanner.
57. Erlandson, R. Finding Help and Keeping Up with Changing Technology in Libraries. *Technology for Small and One-Person Libraries: A LITA Guide* **2013**, *21*, 125.
58. HAFSAOUI, M.A.; MANSOUR, H. D 'e development of a computer park management application. PhD thesis, Universit 'e Virtual of Tunis, 2019.
59. MyLanViewer Network/IP Scanner.
60. Garcia, H.C. About monitoring the confidentiality of computer systems. *Mathematical machines and systems* **2015**.
61. Dandan, T. LAN scan MyLanViewer. *Cyber security and information* **2017**, p. 94.
62. Nessus.
63. Anderson, H. Introduction to nessus. *SecurityFocus. Saatavilla wwwosoitteessa< http://www. securityfocus. com/infocus/1741* **2003**.
64. Wijaya, S.A.A. ATCS System Security Audit Using Nessus. *ATCS* **2017**, *7*.

 doi:10.20944/preprints202505.1028.v1

65. Josephlal, E.F.M.; Adepu, S. Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability. In Proceedings of the 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE). IEEE, 2019, pp. 241–246.
66. Memon, I.; Shaikh, R.A.; Fazal, H.; Tunio, H.; Arain, Q.A. The World of Hacking: A Survey. *University of Sindh Journal of Information and Communication Technology* **2020**, *4*, 31–37.
67. Zhang, W.; Banescu, S.; Pasos, L.; Stewart, S.; Ganesh, V. MPro: Combining Static and Symbolic Analysis for Scalable Testing of Smart Contract. *arXiv preprint arXiv:1911.00570* **2019**.
68. Singh, R.R.; Tomar, D.S. Network forensics: Detection and analysis of stealth port scanning attack. *scanning* **2015**, *4*, 8.
69. Patel, S.K.; Sonker, A. Internet protocol identification number based ideal stealth port scan detection using snort. In Proceedings of the 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2016, pp. 422–427.
70. Coyle, S. Port Scanning Techniques Tools and Detection **2024**.
71. Qureshi, M.A.; Ahmed, S.; Mehmood, A.; Shaheen, R.; Dildar, M.S. Vulnerability assessment of operating systems in healthcare: exploitation implications techniques and security. *Health Sciences Journal* **2024**, *2*, 104–111.
72. Mitre. Common Vulnerabilities and Exposures (CVE). [Accessed: 2020-07-29].
73. Bonandir, A.; Yussof, S. An analysis of common vulnerability and exposure (CVE) of software products in the year 2016. *International Journal of Advanced Science and Technology* **2018**, *112*, 157–166.
74. Firewall.