ISSN 2278-3091
Volume 10, No.6, November - December 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse021062021.pdf
https://doi.org/10.30534/ijatcse/2021/021062021

University Computer Network Vulnerability Management using Nmap and Nexpose

Kismat Chhillar[1], Saurabh Shrivastava[2]
[1]Bundelkhand University,Jhansi, India, ksmtchhillar@gmail.com
[2]Bundelkhand University, Jhansi, India, hanu.saurabh@gmail.com

Received Date : October 07, 2021 Accepted Date : November 04, 2021 Published Date : December 06, 2021

ABSTRACT

Over the past few years, the advancement of technology in universities have led to rise in the number of vulnerabilities in University computer Network (UCN). To ensure robustness and hardness of UCN, an efficient Vulnerability Management System is required. The focus of current work is on the importance of vulnerability management in a UCN. A plethora of tools are used for vulnerability scanning and assessment. This paper also focuses on the implementation of vulnerability scanning tools on UCN. Assessment of scan results is done to identify vulnerabilities in the network that need to be resolved on priority basis. Based on the scan results obtained after scanning the network using scanning tools, the decision can be taken to mitigate the vulnerabilities on priority basis. Vulnerability Management in a UCN is a stepwise procedure that needs to be implemented to keep the network secure. An effective VM framework is important and inevitable to prevent cyber security breaches in a UCN as it regularly checks for new vulnerabilities on and also provide solutions to remediate or resolve the vulnerabilities. The scanning tools used for the current work were Nmap and Nexpose. Nmap was used for information gathering of network and Nexpose was used for scanning the network for vulnerability detection.

Key words: Network Security, Network Vulnerability Assessment, Network Vulnerability Management, Vulnerability Scanning, University Computer Network.

1. INTRODUCTION

To ensure network security, an efficient Vulnerability Management Framework (VMF) has become the need of the hour. The vulnerabilities in a UCN is increasing at a rapid rate which needs to be remediated efficiently and effectively. Network Vulnerability Management (VM) is a cyclic process that deals with identification, classification, prioritization, remediation and mitigation of vulnerabilities in a network. Current paper deals with Vulnerabilities in a UCN. Vulnerabilities are detected and identified by using vulnerability scanners. Such scanners are designed to assess networks, applications and computers for known vulnerabilities. The vulnerabilities of a network can arise from flawed programming or misconfigurations within an asset like router, firewall, application server, web server etc. Vulnerability remediation's may include change in security policy of network, patch installation, educating users about network security and software reconfiguration.

Network VM identifies vulnerabilities in a network and also evaluates the risk associated with these vulnerabilities. This evaluation further helps in mitigation or remediation of vulnerabilities. More is the risk associated with a vulnerability, sooner it needs to be remediated. VM is a broader term as compared to vulnerability scanning. Apart from vulnerability scanning, VM considers other aspects as well like Risk assessment, remediation of vulnerabilities etc.

The rest of the paper is organized as follows. Section 2 deals with important concepts like vulnerability management process, Vulnerability Scanning and Scanning tools. Section 3 discusses about related work that has already been done by various researchers. Section 4 discusses about implementation of vulnerability management and scanning of a University Computer Network (UCN). The implementation of vulnerability scanning tools has been done on Bundelkhand University (Jhansi, India) Computer Network. Section 5 presents scan result analysis and remediation's of vulnerabilities based on VM process. Section 6 discusses about conclusion and future scope of this research.

2. IMPORTANT CONCEPTS

2.1 Vulnerability Management Process (VMP)

To ensure network security in a University Computer Network (UCN), a proper and effective Vulnerability Management Process (VMP) has become inevitable. Vulnerabilities are increasing day by day and being large in number, it is not possible to deal with vulnerabilities manually. This demands for a stepwise and well-planned management of vulnerabilities. All this can be achieved by an

efficient implementation of a VMP. The main objective of a VMP is timely detection and remediation of vulnerabilities. Vulnerability scanning needs to be performed on regular basis to know the state of network and keep a check on vulnerabilities. Timely scanning of network for vulnerabilities is a must to keep the network robust and to ensure confidentiality, integrity and authenticity of network data.

The various phases of a VMP are as follows

- Discovery of Network Assets
- Categorization of Network Assets
- Scanning of Network for Vulnerabilities
- Report Generation
- Analyzing Scan results
- Prioritize remediation's of Vulnerabilities
- Remediate the Vulnerabilities
- Verification and monitoring of Network Security

A VMP is cyclic in nature and above steps are repeated at regular intervals to ensure security and robustness of network. Phases of a VMP are shown in figure 1.

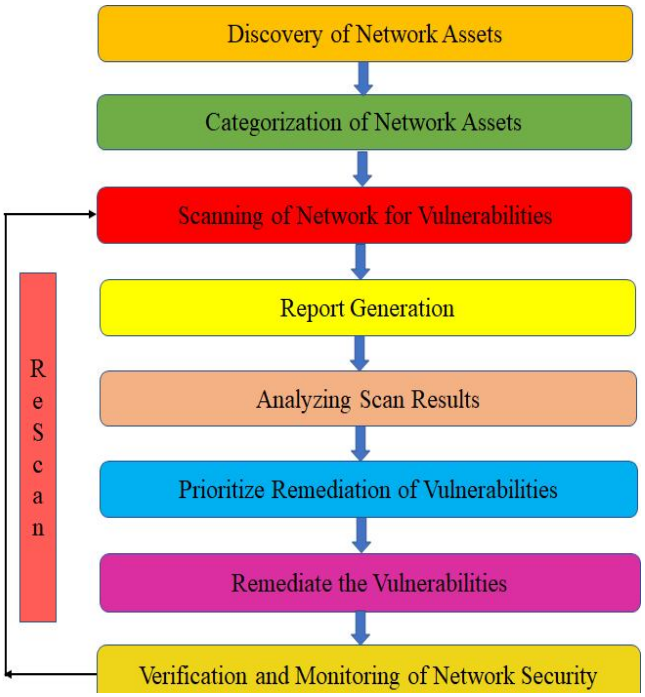

Figure 1: Phases of a VMP

2.2 Vulnerability Scanning and Assessment

Vulnerability Scanning is a process of identifying weaknesses or vulnerabilities in a network. Vulnerability scanning is done with the help of various scanning tools available like Nessus, Nexpose, Qualys, Nmap, Zenmap, OpenVAS etc.The vulnerability scanning steps are vulnerability identification, Analysis of results, risk assessment, remediation and implementation. The scanning steps are followed in cyclic manner as they are repeated at regular intervals to ensure security of network. Vulnerability Assessment is a broader concept as compared to Vulnerability scanning. The vulnerability assessment process is conducted in a stepwise manner. The steps are asset discovery and classification of assets, vulnerability scanning, vulnerability analysis, Prioritization of vulnerabilities, remediation of vulnerabilities and finally verification of vulnerabilities whether they are fixed properly or not.

2.3 Network Scanning Tools

Network scanning tools are of different types. There are tools for network mapping which are used for information gathering of network. Network mapping includes Port scanning, Operating System and Services fingerprinting. Nmap and Zenmap are very efficient tools that can be used for network mapping. For Current work, Nmap has been used for information gathering of network. Zenmap is similar to Nmap but it is GUI version of Nmap. The operating system used for implementation of Nmap is Kali Linux. The vulnerability scanning tools are used to scan network for vulnerability detection. The vulnerability scanner used for this work is Nexpose.

A. NMAP

Nmap stands for "Network Mapper". Nmap is a free and open source tool for discovery of network and auditing of security [1]. Nmap makes use of raw IP packets to determine available hosts on the network. It is used for port scanning to determine open ports on hosts. Nmap also determines the services (name and version of application) offered by the available hosts, the operating systems and the OS versions that are running, the type of firewalls/ packet filters in use. Nmap is a tool that is flexible, easy, portable, powerful, free, supported, well documented, acclaimed and popular. Nmap provides host discovery and detection of services and operating systems. The use of Nmap scripts provides more advanced features of vulnerability detection, service detection and other features. The most important features of Nmap are:

a) Host Discovery
b) Port Scanning
c) Services detection
d) TCP/IP stack fingerprinting
e) Scriptable interaction with hosts

Nmap can also provide information about device types, MAC addresses etc."

B. Nexpose

Nexpose is a scanning tool which detects for open ports, services and running applications. Using the applications and services, it tries to detect vulnerabilities that are existing in a network. After scanning, the scan results are disclosed by Nexpose in the form of a report which helps in prioritizing vulnerabilities based on risk factor and an effective solution is generated to be implemented [2]. Nexpose is a vulnerability scanning tool by Rapid7. Nexpose community edition is free to use but with limited number of assets and scan capabilities and the commercial version is paid. For this work, we have

used Nexpose community edition. The entire VM Lifecycle is supported by Nexpose including discovery of assets, detection of assets, verification, classification of risk, analysis of impact, report generation and mitigation of vulnerabilities [3]. For vulnerability exploitation, Nexpose can be integrated with Rapid7's Matasploit. In Nexpose, user interaction is done through web browser. The login screen after installing and set up of nexpose can be seen in figure 2.

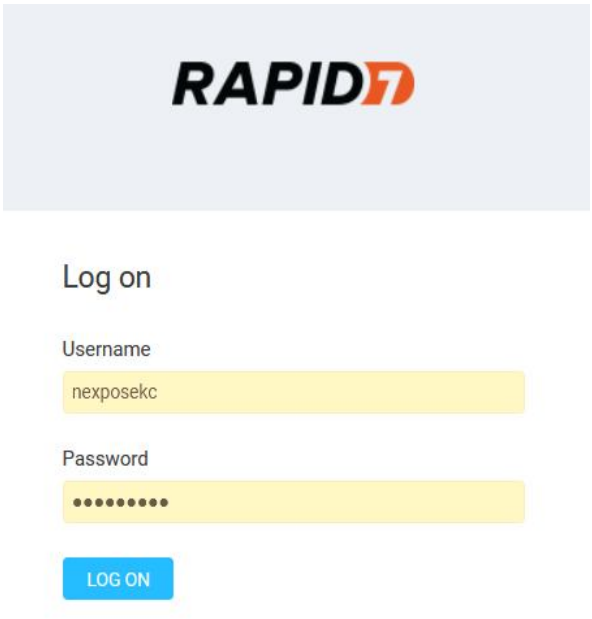

Figure 2: Nexpose Login Screen

The terms that are frequently used in Nexpose is as below.

- Asset
- Site
- Scan Template

Asset refers to host in a network and site is a logical group of assets having a dedicated scan engine. The audit level used by Nexpose to perform a vulnerability scan is defined by a scan template.

3. RELATED WORK

Kumar and Tlhagadikgora [4] in discussed about various tools for vulnerability scanning and exploitation. The authors discussed about penetration testing of internal network using free or open source tools. Nagendram*et. al* [5] utilized cisco packet tracer to evaluate the performance of wide area network. Aksu *et. al* [6] evaluated the usability of an open source vulnerability scanner OpenVAS. They carried out user-based and expert-based testing. Chalvatzis *et. al* [7] provided a framework which is based on virtual machine and used this framework to evaluate the performance of three vulnerability scanners on small and medium sized enterprises. Kumar *et. al* [8] proposed a system for identification, fixing and reporting of vulnerabilities of network over Local Area Network (LAN). The Telnet-SSH connection is automated using Python and is used for vulnerability of physical open ports.

Patil *et. al* [9] discussed about the importance of ethical hacking to ensure cybersecurity. Shah and Mehtre [10] developed a new tool for vulnerability assessment and penetration testing (VAPT). The name of the tool is Net-Nirikshak 1.0 and all the operational and technical aspects of the tool are described by the authors. Based on vulnerability scan, Haifeng Wu in [11] designed a network security assessment system. In this system, the detection is on basis of relational database (RDB) and the method of assessment is based on fuzzy. Pattanavichai in [12] compared the scanning tools for network security. Two tools have been studied namely Microsoft Baseline Security Analyzer (MBSA) and GFI LanGuard. Mandal and Jadhav [13] surveyed about open source network security tools.

4. NETWORK VULNERABILITY SCANNING USING NMAP AND NEXPOSE

4.1Network Information Gathering using Nmap

The implementation of Nmap is done on a few subnets of Bundelkhand University, Jhansi, India. Six subnets were scanned using Nmap. The operating system used for scanning using Nmap is Kali Linux. Kali Linux is an effective and very popular operating system as far as vulnerability scanning and Penetration testing is concerned. Three subnets of Bundelkhand University (BU) Jhansi have been scanned using Nmap. The subnets that were scanned are listed in Table 1.

Table 1: Subnets Scanned using Nmap

Subnet	IP Address
1	172.16.22.1
2	172.16.6.1
3	172.16.3.1

One of the most used and popular Nmap command is PING Scan which is used for detection of hosts on any network. Figure3, 4&5 shows the execution of Nmap PING Scan on subnets selected in our work. Three subnets of BU Jhansi were scanned using this command. The commands are nmap -sp [Target].

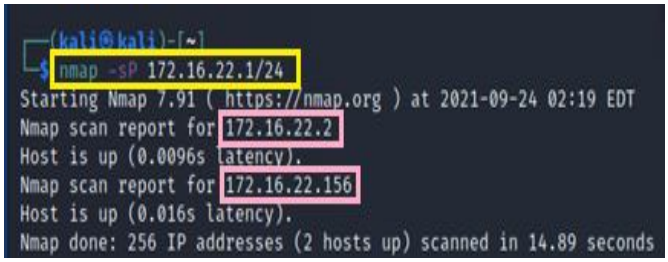

Figure 3: Nmap Scan of Subnet 1

Ping scan results of subnet1 are shown in figure 3. The Ping scan for subnet1 shows that there are 2 hosts up. The subnet is 172.16.22.1/24 and the hosts that are up are 172.16.22.2 and 172.16.22.156.

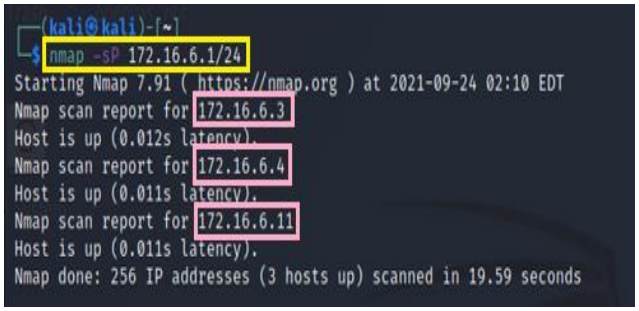

Figure 4: Nmap Scan of Subnet 2

The Ping scan for subnet2 in figure 4 shows that there are 3 hosts up. The subnet is 172.16.6.1/24 and the hosts that are up are 172.16.6.3 and 172.16.6.4 and 172.16.6.11.

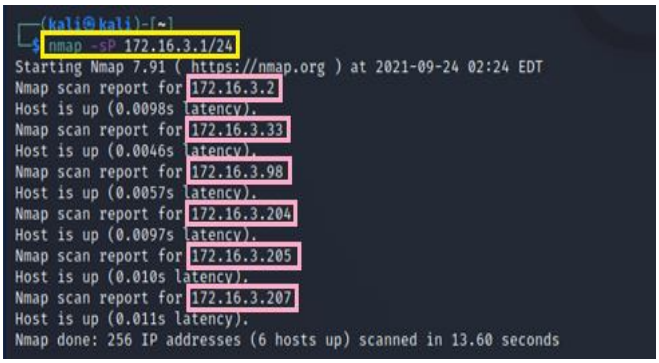

Figure 5: Nmap Scan of Subnet 3

The Ping scan for subnet3 in figure 5 shows that there are 6 hosts up. The subnet is 172.16.3.1/24 and the hosts that are up are 172.16.3.2, 172.16.3.33, 172.16.3.98, 172.16.3.204, 172.16.3.205 and 172.16.3.207.

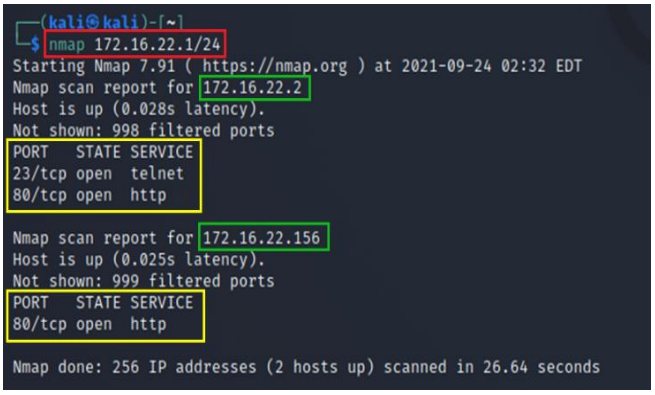

Figure 6: Scan subnet1 using nmap command

Nmap scan of targets give more details as compared to ping scan. The syntax for Nmap command is nmap [Target]. The subnets are scanned using nmap basic command. Figure6, 7 and 8 shows the scan of the targets selected for our work.

The subnet1 scanned shown in figure 6 is 172.16.22.1/24 and there are 2 hosts up.The details of hosts can also be seen in the output. Port, state and service details of hosts can also be known using this scan.

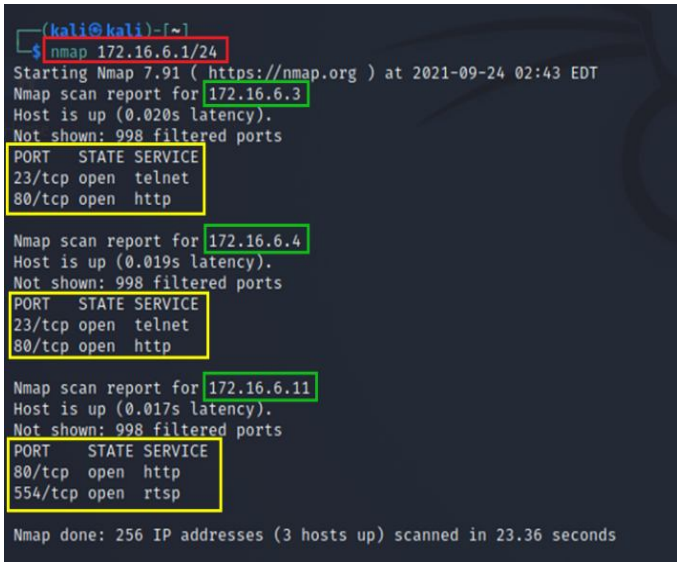

Figure 7: Scan subnet2 using nmap command

Figure7. Shows scan results for subnet 2. Details of each individual host that is up is depicted in the scan output. Subnet2 is 172.16.6.1/24. The host 172.16.6.3, the open ports are port 23 and 80 and the services provided are telnet and http respectively. For host 172.16.6.11, the open ports are 80 and 554 and the services are http and rtsp respectively. Host detail of other subnets can also be seen in similar manner.

Fig 8a and 8b shows scan output of subnet3. There are 6 hosts which are up and details about port, state and service of each host is clearly mentioned in the scan output.

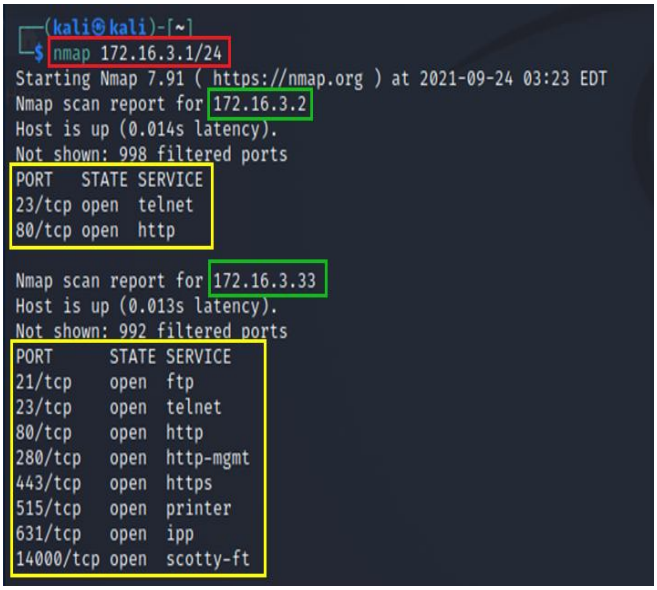

Figure 8(a): Scan subnet3 using nmap command

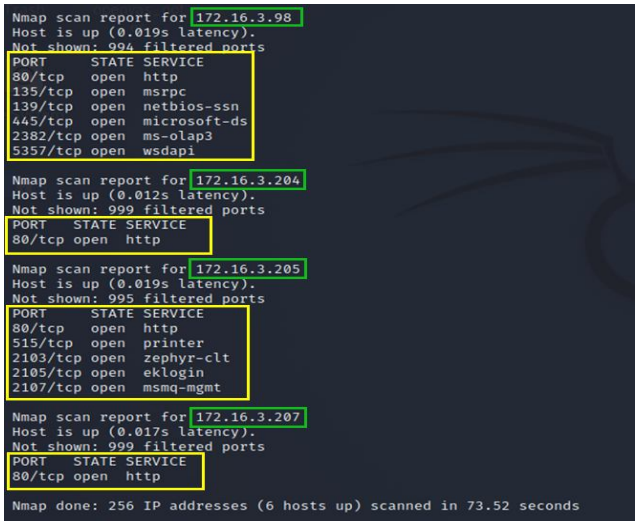

Figure 8(b): Scan subnet3 using nmap command

Port scanning of top 10 ports of a host can be done using the command: nmap -top-ports 10 [Target]. Port Scan of two hosts have beed done. The scan outputs of host1 and host2 are depicted in figure9 and 10 respectively.

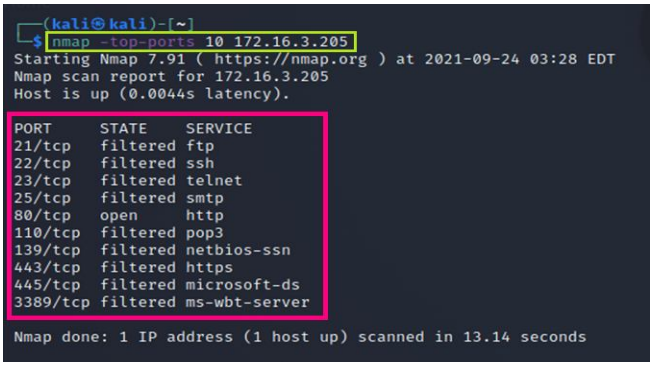

Figure 9: Port Scan of Host1

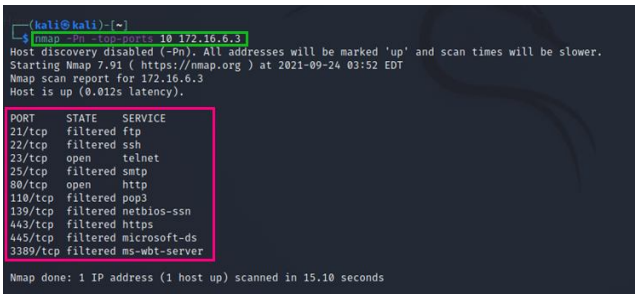

Figure 10: Port Scan of Host2

4.2 Vulnerability Scanning using Nexpose

Three subnets of BU Jhansi were scanned using Nexpose. We need to create a site prior to scan. For site creation there are some settings which we need to complete. For site creation we need to enter details regarding Info & Security, Alerts, Authentication etc. The scan engines, scan templates, scan targets and policies etc. are selected prior to scanning. After entering the details, the site is saved and scanned as per the schedule or it can also be scanned instantly. Figure 11 shows the scan template that we selected while creating site. The scan template that we selected is Full audit without web spider.

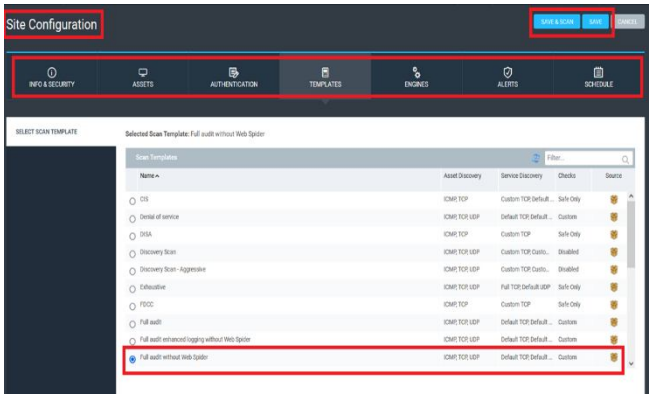

Figure 11: Selecting Scan Template

Figure 12 shows the screenshot of the scan engine that we selected while creating a site. The scan engine that we selected for scanning is Local Scan Engine.

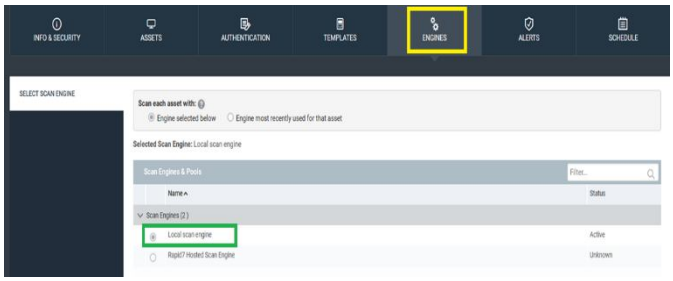

Figure 12: Selecting Scan Engine

5. SCAN RESULT ANALYSIS

From scan results of Nmap and Nexpose, we clearly get an idea about the current state of network that we scanned. Nmap provides information about a network like host details, port details, state of port and services provided etc. Nexpose scan results exposes vulnerabilities present in a network.

Nmap scan results gave us list of ports that were open, closed or filtered. Open ports can be misused by the malicious entities. Filtered ports means they cannot be detected whether open or closed due to presence of a secure medium like firewall etc. Through different commands of Nmap we can easily determine the status of hosts in a network whether the hosts are up or not. If the hosts are up, we can determine the Port name, status and services provided. There are several commands that are used in Nmap to know different details about a network. By running commands as per the requirement gives us clear picture of how secure a network is. By gathering information about a network, network security engineers or security personnel can try to remove the pitfalls of a network before it gets exploited by hackers or entities with malicious intent.

Nexpose scan results provides the vulnerabilities present in the scanned network. Table 2 shows IP address, Number of vulnerabilities detected and risk score of the hosts scanned.

Table 2: Nexpose Scan Result of Hosts

Address	Vulnerabilities	Risk Score
172.16.22.2	3	1311.6533
172.16.22.1	6	4198.7046
172.16.6.172	6	3560.3647
172.16.6.35	17	7803.292
172.16.6.4	3	1311.6533
172.16.6.3	3	1311.6533
172.16.6.171	5	3560.3645
172.16.6.210	8	4479.1147
172.16.6.1	6	4198.7046
172.16.6.32	7	4479.1147
172.16.6.201	9	4311.0176
172.16.3.202	6	3099.5347
172.16.3.33	36	18871.068
172.16.3.1	6	4198.7046
172.16.3.211	1	458.06064
172.16.3.212	11	5927.094
172.16.3.2	3	1311.6533
172.16.3.207	2	1168.7344
172.16.3.205	2	1168.7344
172.16.3.204	2	1168.7344

Figure 13 represents the count of vulnerabilities present in the hosts scanned by Nexpose scanner. From the scan result we can determine the host with the greatest number of vulnerabilities. The host 172.16.3.33 has the highest number of vulnerabilities i: e 36. The host 172.16.6.35 and 172.16.3.212 are also highly vulnerable having vulnerability count as 17 and 11 respectively.

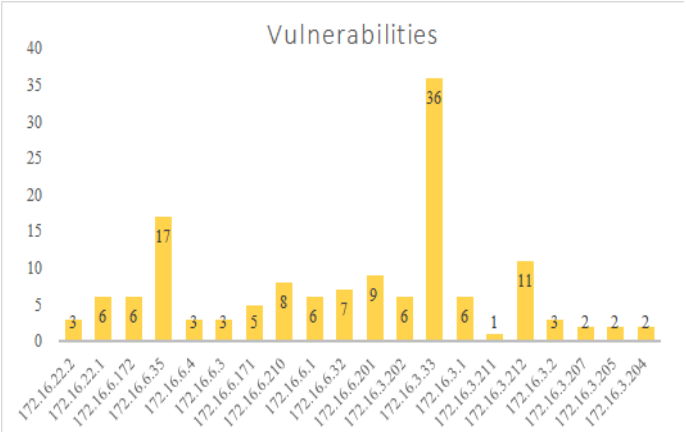

Figure 13: Vulnerability count of hosts scanned

The risk score of the hosts scanned is also determined by Nexpose scanner. Figure 14 presents the risk score of scanned hosts. From the scan results, we can determine the hosts which are at high risk. Host 172.16.3.33 is at the highest risk. This host also has the highest number of vulnerabilities. Hence, there are high chances that the host having high number of vulnerabilities is at a high risk of being exploited by the malicious entities or hackers.

Figure 14: Risk Score of hosts scanned

Based on the number of vulnerabilities and risk score of a host, remediations can be taken on priority basis. The hosts which are at high risk and is highly vulnerable to attacks need to be dealt first. Various other details can also be retrieved from Nexpose scan like CVSS score of vulnerabilities, Operating system detected, malwares etc. This gives a clear picture of how robust and secure is the network.

6. CONCLUSION AND FUTURE WORK

Vulnerability scanning of a University Computer Network (UCN) have been performed using two very popular and efficient scanning tools namely Nmap and Nexpose. Nmap is a network mapper used for gathering information about a

network and Nexpose does the actual task of vulnerability scanning. Scanners are crucial tools for effective Vulnerability Management (VM). The scan results were analyzed to identify the most vulnerable hosts and on the basis of scan results, the prioritization and remediation decisions are taken by the concerned authority. In the future, various other Nmap commands can be used for scanning and different aspects of Nexpose can be utilized for vulnerability scanning to scan a network more efficiently.

ACKNOWLEDGEMENT

I am sincerely thankful to Bundelkhand University Jhansi for assisting me to conduct vulnerability Scanning of UCN. I thank System Analyst of the university for his complete support in conducting my scanning task efficiently.

REFERENCES

1. https://nmap.org/.
2. https://docs.rapid7.com/metasploit/vulnerability-scanning-with-nexpose/.
3. https://sectools.org/tool/nexpose/.
4. R. Kumar and K. Tlhagadikgora. **Internal Network Penetration Testing Using Free/Open Source Tools: Network and System Administration Approach**,*Communications in Computer and Information Science*, vol. 956, 2018. https://doi.org/10.1007/978-981-13-3143-5_22
5. Sanam, Nagendram, P. Sai Anil, E.V.S. Pavan and V. Amarendra. **Performance Evaluation of Wide Area Network using Cisco Packet Tracer**. *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 8, Number 6, pp. 2915-2919, 2019. https://doi.org/10.30534/ijatcse/2019/38862019.
6. M. U. Aksu, E. Altuncu and K. Bicakci. **A First Look at the Usability of OpenVAS Vulnerability Scanner**, in *Workshop on Usable Security (USEC 2019)*, pp. 595-600, 24 February 2019. http://dx.doi.org/10.14722/usec.2019.23026
7. I. Chalvatzis, D. A. Karras and R. C. Papademetriou. **Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment**,in *IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, 2019. http://dx.doi.org/10.1109/ICAICA.2019.8873438
8. B. K. Kumar, N. Raj, J. Dhivvya and D. Muralidharan, **Fixing Network Security Vulnerabilities in Local Area Network**, in *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019. http://dx.doi.org/10.1109/ICOEI.2019.8862634
9. S. Patil, A. Jangra, M. Bhale, A. Raina and P. Kulkarni.**Ethical hacking: The need for cyber security**,in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI 2017)*, 2017. doi: 10.1109/ICPCSI.2017.8391982
10. S. Shah and B. Mehtre. **An automated approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0**,in *IEEE International Conference on Advanced Communications, Control and Computing Technologies*, 2014. doi: 10.1109/ICACCCT.2014.7019182
11. H. Wu. **Research of Network security Assessment System based on scan**, in*3rd International Conference on Advanced Computer Control*, 2011.
12. S. Pattanavichai. **Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA)**, *in15th International Conference on ICT and Knowledge Engineering (ICT&KE)*, 2017. doi: 10.1109/ICTKE.2017.8259628
13. N. Mandal and S. Jadhav. **A survey on network security tools for open source**, in *IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, 2016. doi: 10.1109/ICCTAC.2016.7567330