Vulnerability Scanning of University Computer Network Using Zenmap

Kismat Chhillar [1] *and Saurabh Shrivastava* [2]

Abstract

University computer networks have become vast and deal with a lot of critical and sensitive data. This demands the university network to be highly secure. To attain network security, timely assessment of network vulnerabilities has become highly indispensable. The vulnerabilities need to be discovered and removed at the earliest as these can be exploited by attackers having malicious intent. To identify network vulnerabilities, various vulnerability scanning tools are available. The present paper deals with an open source tool ZENMAP which is completely free to use. ZENMAP is the GUI (Graphical User Interface) of Nmap. ZENMAP runs Nmap in the background. Nmap (Network Mapper) is a powerful tool to gather information about any network and its individual devices. This paper describes the implementation of ZENMAP on a few hosts of Bundelkhand University computer network to gather necessary information about the hosts. After knowing the loopholes in a host, measures can be taken to remove the loopholes and enhance network robustness and security.

Keywords : **Computer Network, University Network, Vulnerability assessment, Vulnerability scanning, Zenmap**

I. INTRODUCTION

To ensure network security in universities, vulnerability scanning needs to be done at regular intervals. To ease the task of identifying vulnerabilities, various vulnerability scanning tools are available. A vulnerability scanner is a tool that identifies vulnerabilities or weaknesses in a network or any host. Every scanner performs scans differently and provides scan results that aid in taking further actions regarding remediations and making the network more robust and reliable.

There are many tools available for vulnerability scanning. In this work we will be discussing about working of Zenmap. Zenmap in nothing but Nmap in the background. Zenmap performs the task of network mapping. In this paper, we will be discussing the implementation of Zenmap on a few live hosts of a subnet of Bundelkhand University, Jhansi. After analyzing the scan results, we can infer whether the hosts are safe or vulnerable to attacks.

Scanning tools are highly effective in identifying vulnerabilities in a network and also provide remediations to get rid of any particular vulnerability.

Section II of the paper discusses important concepts that we need to know prior to performing the actual task of scanning. Section III discusses the methodology of vulnerability scanning. Section IV shows the actual implementation of Zenmap on a few live hosts of Bundelkhand University, Jhansi. Section V covers scan results and analysis of the results. Finally, section VI discusses the conclusion and future scope of the current work.

Manuscript Received : September 20, 2021; Revised : October 19, 2021 ; Accepted : October 24, 2021. Date of Publication : December 5, 2021.

K. Chhillar[1] is *Research Scholar* with Department of Mathematical Sciences & Computer Application, Bundelkhand University, Jhansi, Uttar Pradesh - 284 128. Email : chhillarkismat1@gmail.com ; ORCID iD : https://orcid.org/0000-0003-0538-8158
S. Shrivastava[2] is *Associate Professor* with Department of Mathematical Sciences & Computer Application, Bundelkhand University, Jhansi, Uttar Pradesh - 284 128.
Email : hanu.saurabh@gmail.com ; ORCID iD : https://orcid.org/0000-0002-7793-1861

DOI : https://doi.org/10.17010/ijcs/2021/v6/i6/167640

II. IMPORTANT CONCEPTS

A. Vulnerability

Vulnerability refers to any weakness or loophole in a device or network that can be taken advantage of. Vulnerability can be software vulnerability, computer system vulnerability, network unit vulnerability, and information systems vulnerability. This work focusses on network vulnerability assessment.

"A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach" [1].

Network unit vulnerability means any weakness or loopholes in the computer network or any hosts in the network. These vulnerabilities can be exploited by the attackers. Through these vulnerabilities, attackers try to access the network and gain unauthorized access to the network to implement their malicious intent.

B. Network Vulnerability Assessment

A network vulnerability assessment is identifying vulnerabilities in a network through scanning the network and analyzing the scan results to look for vulnerabilities and remediating those vulnerabilities depending on the severity/criticality of that vulnerability. Critical vulnerabilities possess greater risk to the entire network. Hence, they need to be got rid of at the earliest.

The steps of network vulnerability assessment process are as follows:

- Conduct risk identification and analysis
- Vulnerability scanning policies and procedures
- Identifying the type of vulnerability scans
- Configure the scan
- Perform the scan
- Evaluate and consider possible risks
- Interpret the scan results
- Create a remediation process and mitigation plan

There are enormous benefits associated with performing regular vulnerability assessments. Many security experts suggest performing vulnerability assessments atleast quarterly.

C. Zenmap

Zenmap is the GUI version of Nmap. Nmap works in the background. Zenmap is multi-platform and makes Nmap easy to use. It is an open source and free to use application. Nmap stands for Network mapper. Zenmap also provides advanced features for the experienced. Scan results can be saved and they can be viewed any time.

III. RELATED WORK

Researches have been done in the past by many researchers regarding network scanning and vulnerability assessment tools. Wang, Liu, Li, Zhang, Chen, and Zou [2] elaborated vulnerability scanning technology and web application security. Khavya and Hema Priya [3] surveyed security assessment and forensic analysis related to android m-banking applications. Shah, Ahmed, Saeed, Junaid, Khan, and Ata-Ur-Rehman [4] proposed scan strategy on how penetration testing deals with large volume of class A and class B hosts.

Mandal and Jadhav [5] presented an overview of threats and attacks on a network. This paper discussed various open source tools like Tcpdump, Nmap, Wireshark, and Firewall. Bhanu Prakash and Reddy [6] discussed about cyber-attacks, cyber security, and cyber laws. Authors also emphasized the importance of legal framework to deat with cyber frauds and cyber-attacks. Wang, Bai, Li, Chen, and Chen [7] designed a network vulnerability scanning system. This system is based on NVTs and also conducted a test for this system. Alzahrani [8] proposed a network security penetration tool that used Nessus and Metasploit to detect vulnerabilities in the network and used the tool to increase the overall performance and security of Albaha University network.

Gbedawo, Agbesi, and Adukpo [9] conducted penetration test that simulated intrusion detection using free and open source software tools (FOSS). Some of the tools that were used for this are Zentyl server, VMware Fusion, Suricata, OpenVAS, and Metasploit Framework. Raza, Maliyekkal, and Choudhary [10] discussed scanning an organization's internal network using Raspberry Pi. This work also used tools like Nmap and Nikto. Kaur and Kaur [11] performed penetration testing on a target operating system to find security vulnerabilities. Nmap tool was used for reconnaissance or information gathering phase.

Tundis, Mazurczyk, and Mühlhäuser [12] reviewed various scanning tools used for network vulnerability scanning and also discussed about their types, functioning, and capabilities. Dinh, Xuan, Thai, Pardalos, and Znati [13] proposed vulnerability assessment framework and also proposed approximation algorithm. They discussed new approaches for vulnerability assessment. Schagen, Koning, Bos, and Giuffrida [14] implemented a framework for scanning of vulnerabilities of network servers.

IV. ZENMAP IMPLEMENTATION

Zenmap is the graphical user interface of Nmap. It is used to gather information about any host in a network just by knowing its IP address. It can bypass security measures like firewall.

Zenmap features are as follows:

- It is interactive and used for graphical results viewing.
- It can be used to compare two scan results.
- Zenmap scan commands can be run repeatedly.
- It is easy and convenient to use.

When the Zenmap is opened, the first screen looks like as shown in Fig. 1. In target fields we can enter the IP addresses to be scanned. From profile dropdown we select the profile. The command field shows the command that is used for scanning. Target to be scanned is entered in the target field and profile is selected. Various scan profiles are available in Zenmap as shown in Fig. 2. Any number of targets can be scanned by entering them in the targets field but they need to be separated by spaces.

A subnet of Bundelkhand University, Jhansi is

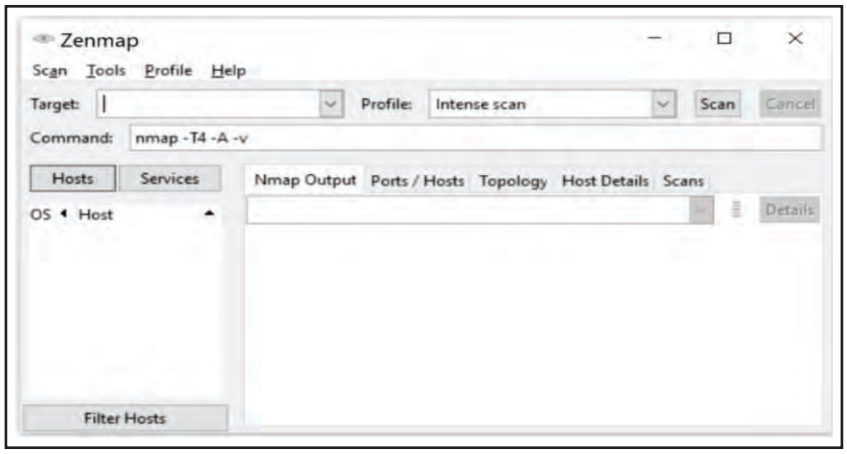

Fig. 1. Initial Screen of Zenmap

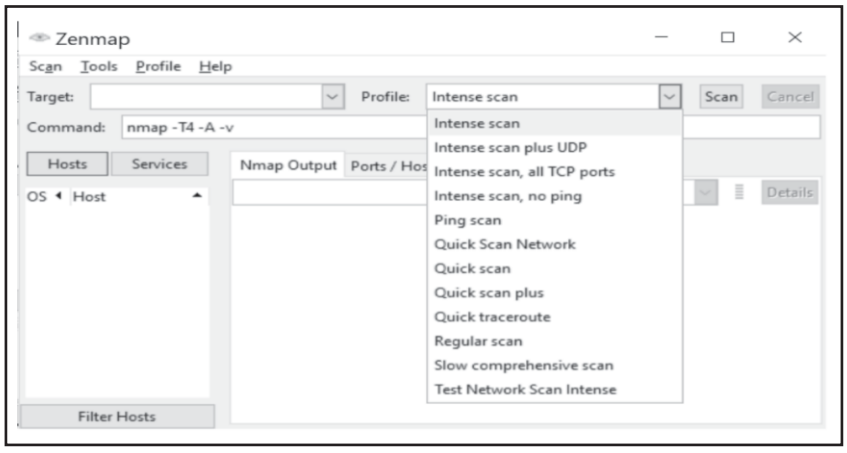

Fig. 2. Different Scan Profiles in Zenmap

scanned using different scan profiles of Zenmap. The subnet scanned is entered in the target fields and scan results are analyzed to know the security of the network.

The scan profiles selected for the present study are ping scan, quick scan, quick scan plus, intense scan, and regular scan. Every scan is different. As the scan complexity increases, it covers more details about the target. The scan output displays details about hosts and services available. Ports open for a particular host can also be seen. The services running on a particular port are also included in the scan results.

In the command scan we can see the command for a particular scan. The first scan that we performed is ping scan for which the command is nmap -sn target.

The ping scan command is nmap - sn <target>. The output of ping scan is shown in Fig. 3. Ping scan doesn't perform any port scan, it only pings on the targets. Nmap sends packets to the hosts during this scan and the hosts which respond to the packets are displayed as output of ping scan. Ping scan doesn't show much details. So other scans are also performed to get more details about the hosts.

The next scan that we performed is quick scan. It is slower than ping scan but a bit more detailed than ping scan. The command for quick scan is nmap - T4 - F <target>. It is a fast scan because it scans only top 100 most common tcp ports. The output of quick scan is shown in Fig. 4. To get further details about hosts we performed some other scans also. They are complex as compared to ping scan and quick scan, but to dive deep into further details these scans are necessary.

The next scan that we performed is quick scan plus.

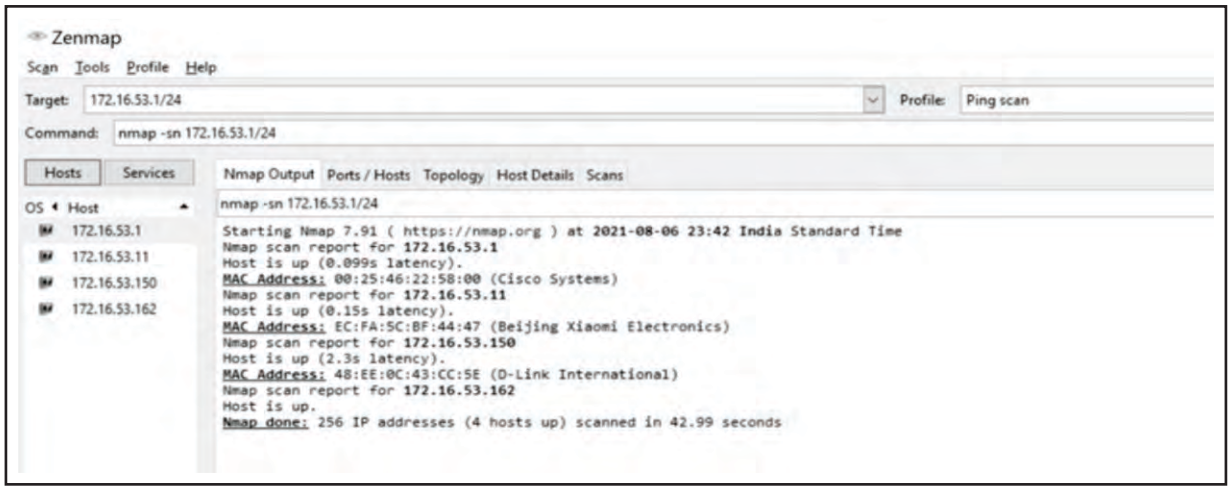

Fig. 3. Ping Scan

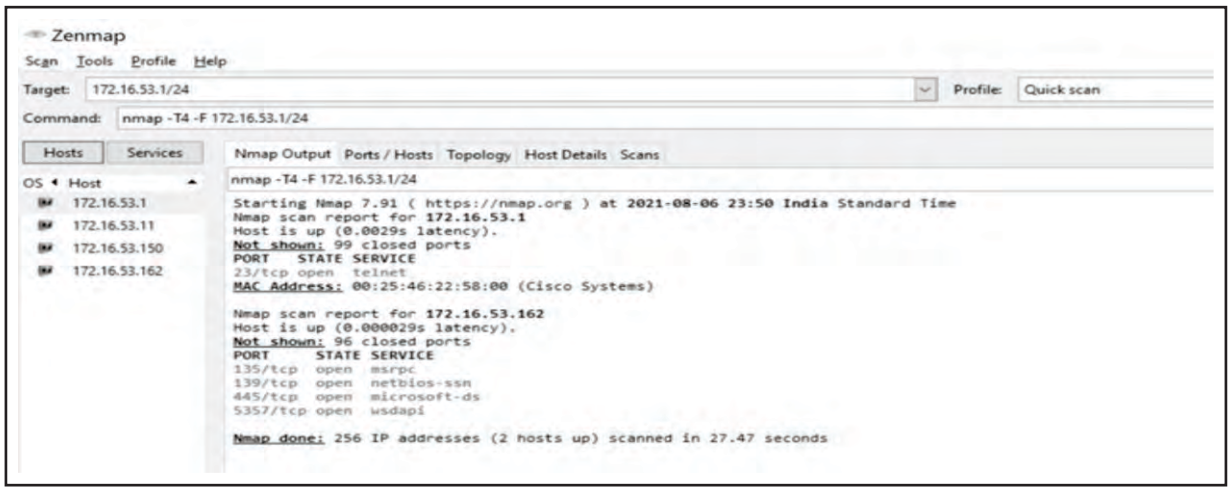

Fig. 4. Quick Scan

The command for this scan is nmap - sV - T4 - O - F --version-light <target>. It is a bit more detailed than previous scans. It also displays Operating System of the host. The scan output is shown in Fig. 5. We can see port, state, service, version, mac address, device type, operating system details, and network distance in the output screen of this scan.

The last scan that we performed for the present work is the Intense scan. The command for this scan is nmap -T4 -A -v <target>. The output is shown in Fig. 6.

Fig. 5. Quick Scan Plus

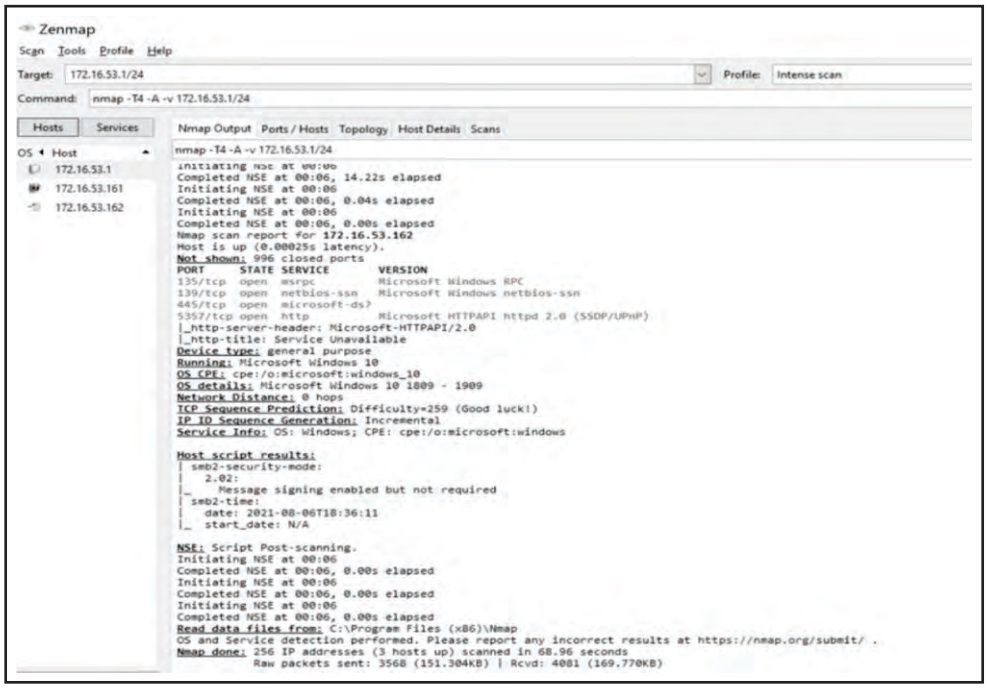

Fig. 6. Intense Scan

V. SCAN RESULT ANALYSIS

Here we will be discussing about Scan results of different scan policies selected. Each scan window has five tabs "Nmap output", "Ports/Hosts", "Topology", "Host Details", "Scans". These tabs are shown in Fig. 7.

Ping scan takes less time to scan and doesn't show detailed information about hosts connected in a network. Only connected devices are shown on the left-hand panel and output shows IP address, MAC address, and vendor of each host.

Now, for quick scan further details about hosts are shown. The important details are highlighted in Fig. 9.

For a particular host, we can see the Ports/Hosts tab in

Fig. 7. Scan Output Tabs

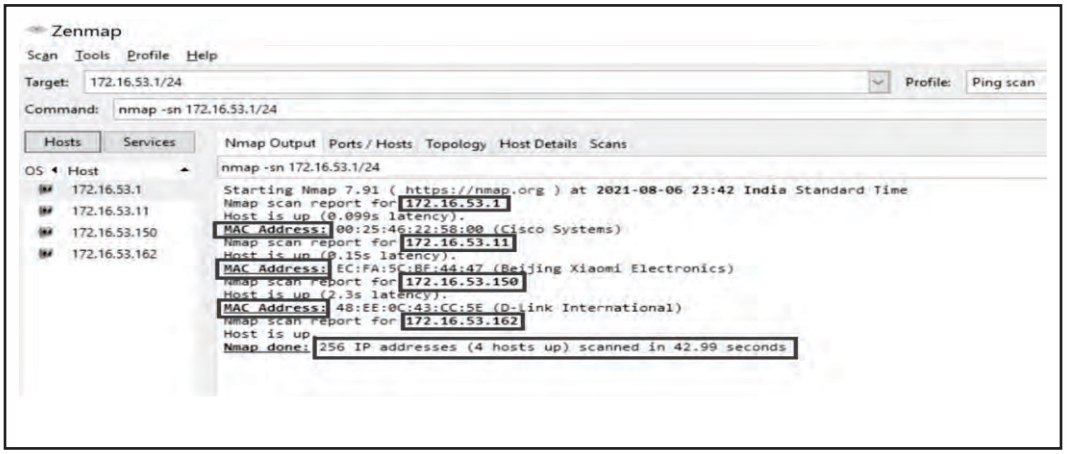

Fig. 8. Ping Scan Results

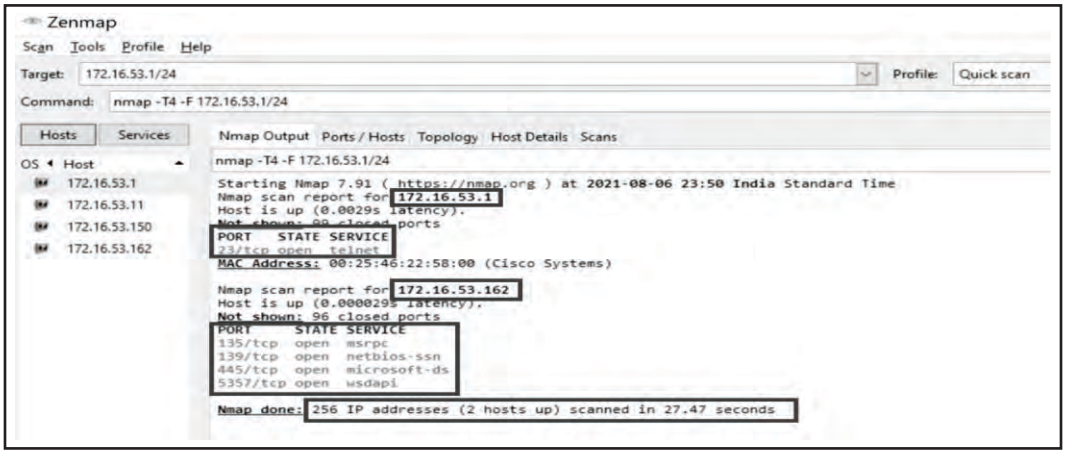

Fig. 9. Quick Scan Results

the scan output window. As shown in Fig. 10, we can get the details of port, protocol, state, service, and version.

The topology tab of output window displays the interactive view of hosts in a network and their connections.

Host details displays information about a host such as the hostnames and addresses, number and status of scanned ports, its state (up or down), the number and status of scanned ports, etc. Fig. 12 shows details about a host scanned. Status is up, open ports 4, IP address, number of scanned ports etc.

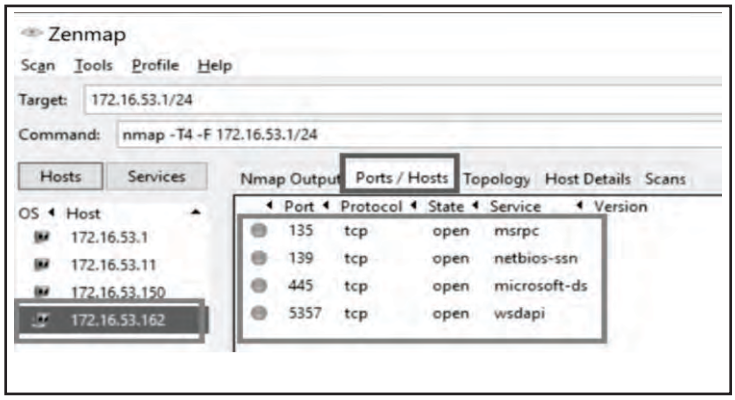

Fig. 10. Quick Scan Results Ports/Hosts Tab Output

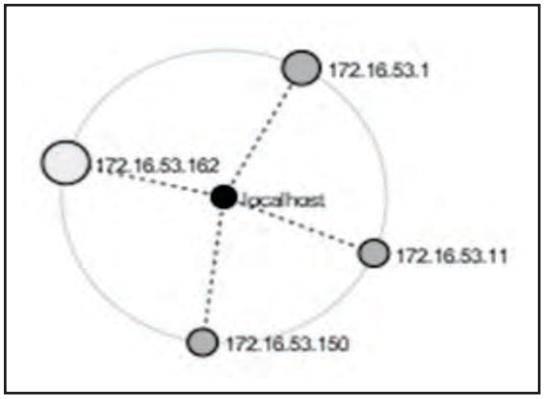

Fig. 11. Quick Scan Result Network Topology

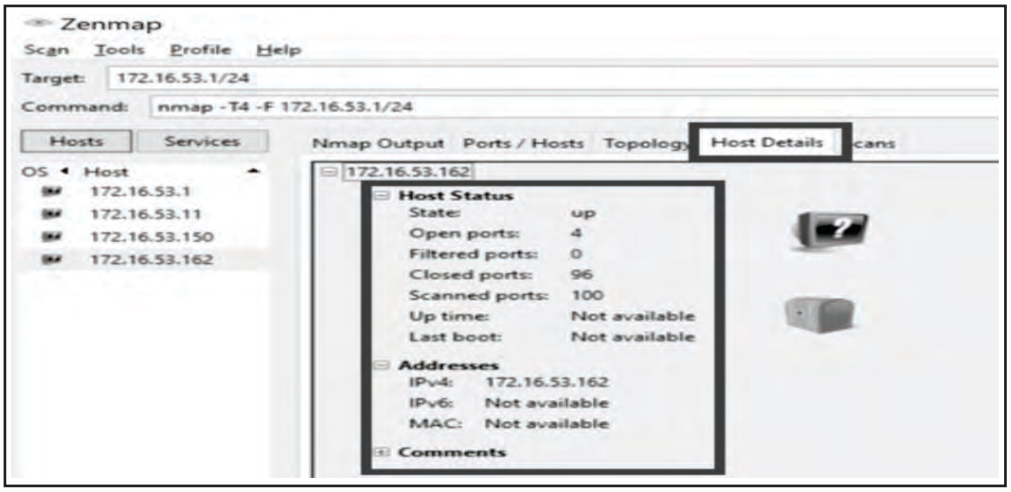

Fig. 12. Host Details Quick Scan

The next scan is quick scan plus. Here, we can see the details of a host as shown in the output. For each host the details shown are IP address, host status, ports details, state, service, version, MAC Address, device type, Operating system details, and network distance.

Host details of quick scan plus displays host status, address, operating system details etc. The operating system used by the host here is Windows 10. Windows icon is also displayed in the scan results.

The last scan performed for the current work is intense scan. The extra details that this scan covers about a host are TCP sequence prediction, IP ID sequence generation, and service info.

From different types of scan in Zenmap, we get a lot of information about a network and an individual host. From the scan results of a host, we get to know the vulnerabilities present in a host like open ports, services running etc. These vulnerabilities need to be removed before being exploited by the malicious entities or hackers. As the complexity of a scan increases, more detailed information about a host can be gathered. After knowing the details of hosts in a network, the IT personnel or the concerned authority dealing with system vulnerabilities can take decisions about remediations of vulnerabilities on a priority basis.

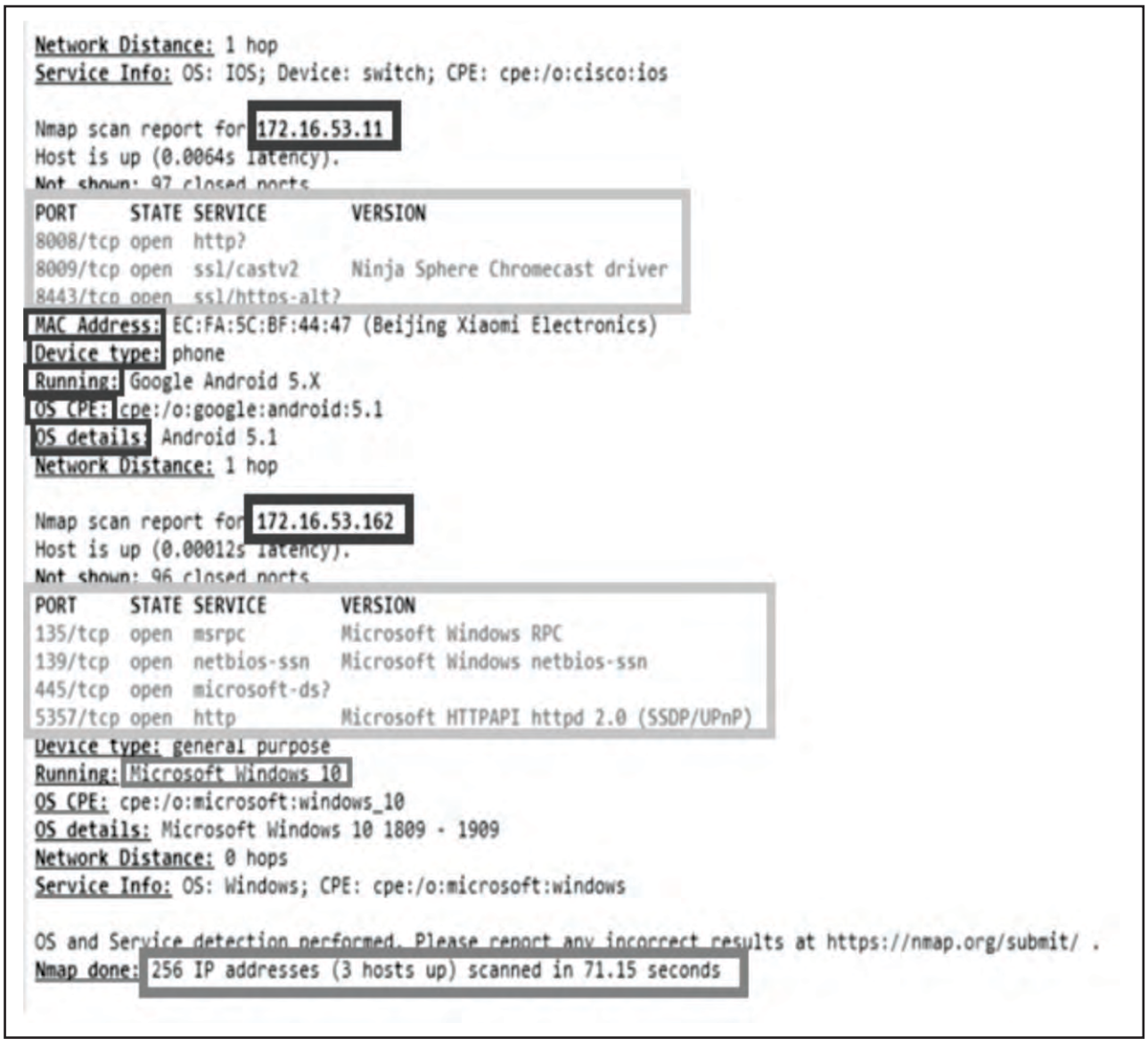

Fig. 13. Quick Scan Plus

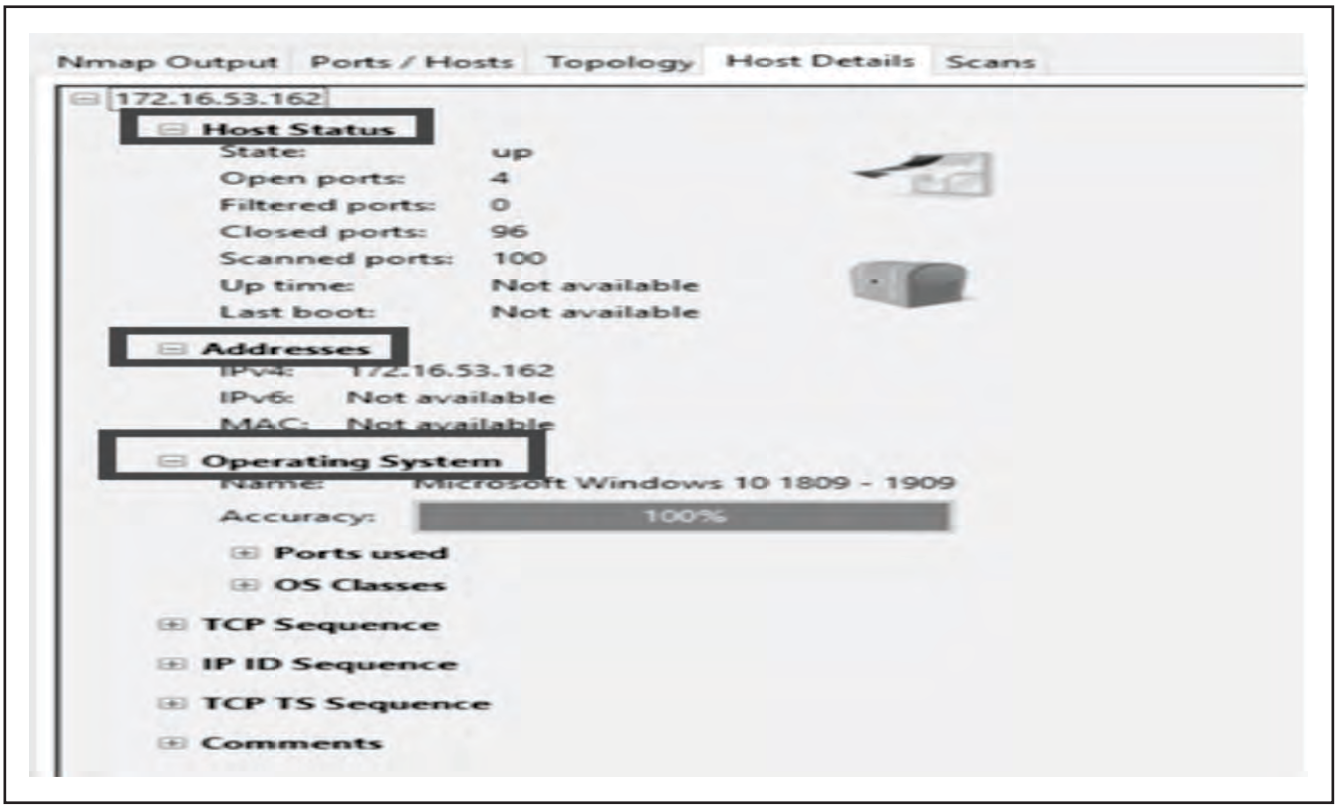

Fig. 14. Quick Scan Plus Result Host Details

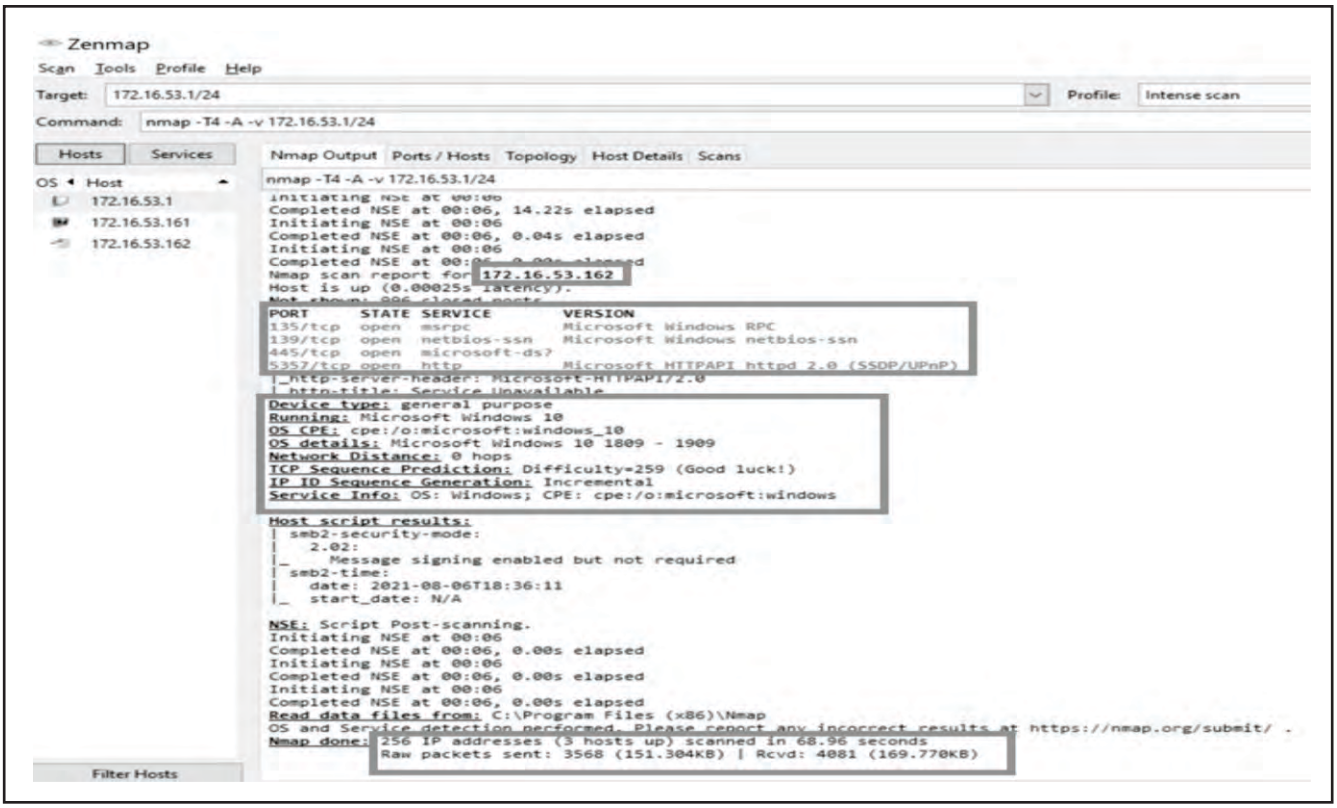

Fig. 15. Intense Scan Results

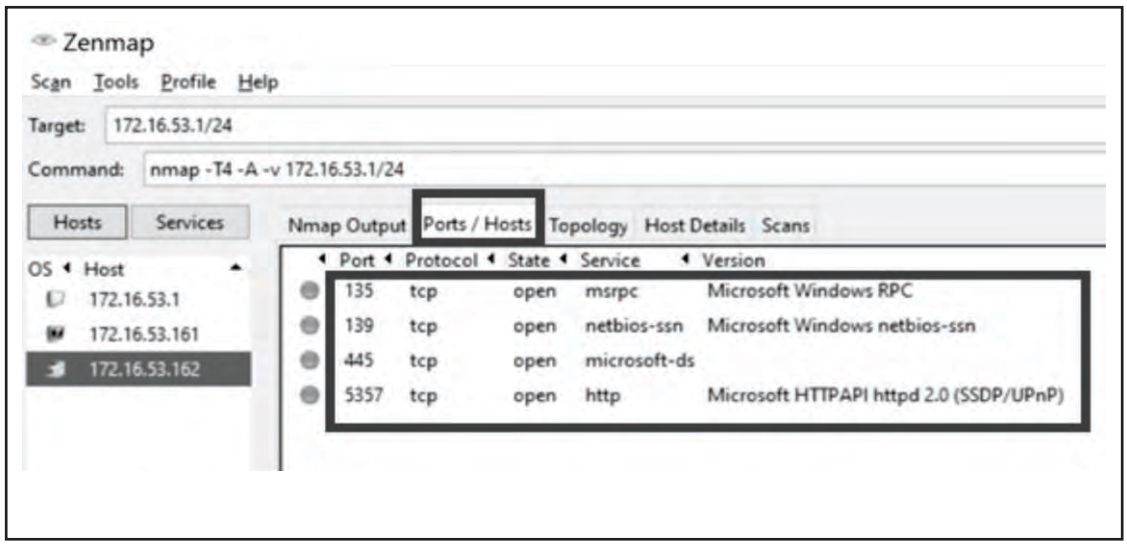

Fig. 16. Intense Scan Ports/Hosts Details

VI. CONCLUSION AND FUTURE SCOPE

The present work scanned a subnet of Bundelkhand University Computer Network. Zenmap Scanner was used for scanning the network. Zenmap is a user-friendly tool. Different scan showed various details about the network. We could generate details about a particular host. Based on scan results we get a clear picture of network and its security. Ports and services are displayed. We can close the open ports which pose threat to network security. Future work can be implementation of more vulnerability scanning tools like Nmap, Qualys, Nessus, Wireshark, Nexpose etc. to scan the network to know it better and detect vulnerabilities in the network so that timely remediations can be taken to get rid of vulnerabilities and make the network highly secure.

ACKNOWLEDGEMENT

The authors are sincerely grateful to Bundelkhand University, Jhansi for allowing them to conduct vulnerability scanning on computer network of the university. They would like to thank the University System Analyst for his complete support in conducting the tasks conveniently and successfully.

AUTHORS' CONTRIBUTION

Both the authors had been actively involved in the presented work. Kismat Chhillar worked on implementation of scanning tool Zenmap on the university computer network. She read the mentioned references and analyzed the scan results obtained from scanning with Zenmap scanning tool. Saurabh Shrivastava closely monitored each step in this work and synergistically helped as a mentor in bringing the desired outcome.

CONFLICT OF INTEREST

The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in the manuscript.

FUNDING ACKNOWLEDGEMENT

The authors received no financial support for the research, authorship, and/or for the publication of the article.

REFERENCES

[1] J. Firch, "Common types of network security vulnerabilities in 2021." Purplesec. https://purplesec.us/common-network-vulnerabilities/

[2] B. Wang, L. Liu, F. Li, J. Zhang, T. Chen, and Z. Zou, "Research on web application security vulnerability scanning

technology," in *2019 IEEE 4th Advanced Inform. Technol., Electron. and Automation Control Conf.,* Chengdu, China, Dec. 20-22, 2019, pp. 1524–1528, doi:10.1109/IAEAC47372.2019.8997964

[3] K. Khavya, and N. H. Priya, "Forensic analysis and security assessment in Android m-Banking applications: A survey." *Indian J. Comput. Sci.,* vol. 4, no. 5, pp. 25–28, Sep. - Oct. 2019, doi: 10.17010/ijcs/2019/v4/i5/149457

[4] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-rehman, "Penetration testing active reconnaissance phase – Optimized port scanning with Nmap tool," in *2nd Int. Conf. Computing, Mathematics and Eng. Technologies (iCoMET),* Sukkur, Pakistan, Jan 30-31, 2019, pp. 1–6. doi: 10.1109/ICOMET.2019.8673520

[5] N. Mandal and S. Jadhav, "A survey on network security tools for open source," in *IEEE Int. Conf. Current Trends Advanced Computing (ICCTAC),* Bangalore, India, 2016, Mar. 20-11, pp. 1–6, doi: 10.1109/ICCTAC.2016.7567330

[6] K. Bhanu Prakash and P. Reddy, "Cyber laws and cyber security : The jurisprudence and judicature," *Indian J. Comput. Sci.,* vol. 3, no. 6, Nov.-Dec. 2018, doi: 10.17010/ijcs/2018/v3/i6/141445

[7] Y. Wang, Y. Bai, L. Li, X. Chen, and A. Chen, "Design of network vulnerability scanning system based on NVTs," In *2020 IEEE 5th Inform.Technol. and Mechatronics Eng. Conf. (ITOEC),* Chongqing, China, Jun.12-14, 2020, pp. 1774–1777, doi: 10.1109/ITOEC49072.2020.9141812.

[8] M. E. Alzahrani, "Auditing Albaha University network security using in-house developed penetration tool," *J. Physics: Conf. Ser.*, vol. 978, Mar. 2018, Art. no. 012093, doi:10.1088/1742-6596/978/1/012093. [Online]. Available: https://ui.adsabs.harvard.edu/link_gateway/2018JPhCS.978a2093A/abstract.

[9] V. Gbedawo, K. Agbesi, and T. Adukpo, "Intrusion detection on campus network, the open source approach: Accra technical university case study," *Int. J. Comput. Appl.,* vol. 164, no. 6, pp. 20–27, Apr. 2017, doi: 10.5120/ijca2017913664

[10] S. Raza, F. J. Maliyekkal, and N. Choudhary, "Remotely scanning organization's internal network," *Int. J. Trend Scientific Res. and Develop.,* vol. 4, no. 6, pp. 1139–1141, Sep.-Oct.2020.[Online].Available: https://www.ijtsrd.com/papers/ijtsrd33636.pdf

[11] G. Kaur and N. Kaur, "Penetration testing – reconnaissance with NMAP tool," *Int. J. Advanced Res. Comput. Sci.,* vol. 8, no. 3, 2017. [Online]. Available: http://www.ijarcs.info/index.php/Ijarcs/article/view/3111

[12] A. Tundis, W. Mazurczyk, and M. Mühlhäuser, "A review of network vulnerabilities scanning tools: Types, capabilities and functioning," In *Proc. 13th Int. Conf. Availability, Rel. and Security (ARES 2018) Assoc. Computing Machinery,* New York, USA, Aug. 2018, pp. 1–10, Art. no. 65, doi: 10.1145/3230833.3233287

[13] T. N. Dinh, Y. Xuan, M. T. Thai, P. M. Pardalos, and T. Znati, "On new approaches of assessing network vulnerability: Hardness and approximation," in *IEEE/ACM Trans. Networking,* vol. 20, no. 2, Apr. 2012, pp. 609-619, doi: 10.1109/TNET.2011.2170849

[14] N. Schagen, K. Koning, H. Bos, and C. Giuffrida, "Towards automated vulnerability scanning of network servers," in *EuroSec'18: Proc. 11th Eur. Workshop Syst. Security,* Porto, Portugal, no. 5, pp. 1-6, Apr. 2018, Art no. 5, doi: 10.1145/3193111.3193116

About the Authors

Kismat Chhillar completed graduation from Miranda House, University of Delhi. Then she did M.C.A. from Aligarh Muslim University. Presently, she is pursuing Ph.D. in Computer Science from Bundelkhand University, Jhansi, Uttar Pradesh.

Saurabh Shrivastava is working as Associate Professor (Computer Science) with Bundelkhand University, Jhansi and has teaching experience of more than 22 years.