

Journal Scientific and Applied Research, Vol. 30, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

IMPLEMENTATION OF MODERN SOFTWARE TOOL FOR CHECKING OPEN PORTS IN THE LOCAL AREA NETWORK

Petar K. Boyanov

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: petar.boyanov@shu.bg

Abstract: *In this scientific article implementation of modern software tool for checking open ports in the local area network is made. Various types of network scans for open ports in a controlled personal lab test environment were performed. Finding open ports helps network administrators identify possible security risks on network devices.*

Key words: *Analysis, Linux, Monitoring, Naabu, Nmap, Ports, Python3, Scanning, Security, Service, Vulnerability, Windows.*

1. Introduction

Naabu is a tool used for network scanning and checking open ports. Its main purpose is to find open ports on an IPv4 or IPv6 address. It helps users to see which services are available on a network. The tool was designed to scan ports quickly and easily. It is often used in network security tests [1,2,3].

Naabu can scan one or several IP addresses at once. It can also scan a full range of IPv4 or IPv6 addresses. One of its main advantages is its speed. It can scan many ports in a short time. The tool uses different scanning methods, but TCP scanning is one of the most common ways to find open ports [4,5,6,10]. Users can also choose a specific list of ports they want to scan. This option is useful when only specific ports need to be checked. This makes the scan faster and avoids checking unnecessary ports [5,6,11].

After the scan is finished, Naabu displays the open ports and the IP addresses where they were found. The ordinary users can also save the results to a file for later analysis. The tool Naabu can also work with other security tools [5,8,9,11]. For example, after finding an open port, another program can be used to check which service is running on it. This provides more details about the network and its active services and current states [1,2,3].

Naabu can be used by both beginners and more experienced users. The program works through the command line, where users enter the IP address, ports and scanning options. It does not have a graphical interface, but its basic commands are not difficult to understand [8,9,10,11]. The users should scan only their own networks or systems for which they have permission. **The content of this academic article is intended for research, instructional**

applications and educational purposes only. Any unauthorized or unethical use of the presented material falls outside the author's scope of responsibility.

2. Related work

Several studies examine network security and methods for finding weaknesses in computer systems. Agrawal et al. [1] describe a framework for testing web application security and finding vulnerabilities. Annaufal et al. [2] test website security using penetration testing methods. Other studies describe automated tools for scanning systems and finding security problems [3,6]. Some studies examine how artificial intelligence can improve penetration testing and speed up security checks [4,5,7,8]. Varma et al. [9] present ReconMaster, a command-line tool for collecting information about websites and network resources. Other studies examine network mapping and system monitoring, which help administrators understand and improve network security [10,11].

3. Problem description and results

The experiments in this study in a controlled personal lab test environment were carried out. The used operating system is Kali linux x64 with the following system information: Linux Petar 7.1.5+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 7.1.5-1kali1 (2026-07-29) x86_64 GNU/Linux.

Naabu and Nmap are two tools used for network scanning and finding open ports. Both tools are used for network security testing, but they offer different features and scanning methods [2,4,5,8,10].

Naabu is designed to find open ports quickly. ts main advantage is its speed when scanning many IPv4 or IPv6 network addresses. Naabu is useful when open ports need to be found quickly. It can also work with other security tools and can be used in automated scans [5,6,7,9].

Nmap is a well-known network scanning tool that has been available for many years. It offers more options for detailed network scanning. Besides finding open ports, it can also identify running services, their versions and sometimes the operating system of the scanned device. Nmap supports several scanning methods and provides additional options for detailed network analysis [3,5,6,10,11].

Naabu is faster than Nmap when the task is to find open ports. Naabu mainly scans for open ports and can check many IPv4 and IPv6 addresses in a short time. This is useful when fast scan results are needed. Naabu is not better than Nmap in every situation [1,2,3,4,11]. Nmap gives more details about scanned devices, while Naabu mainly finds open ports. The two tools can also be used together. For example, Naabu can first find open ports. Nmap can then provide more details about the services running on those ports [7,8,9,10,11].

The IPv4 address of the attacking host in the personal controlled laboratory environment is 192.168.1.18/24 (fig. 2), and the IPv4 address of the victim host is 192.168.1.19/24 (fig. 1). The attacking host uses the Kali Linux operating system, and the victim host uses Microsoft Windows 10. The local test network also contains several other computers. Several servers are installed on the victim host which are respectively:

- Apache server with ports 80 and 443;
- MySQL server with port 3306;
- FileZilla server with ports 21 and 14147;
- Mercury server with ports 25, 79, 105, 106, 110, 143 and 2224;
- TomCat server with ports 8005, 8080, 49674 and 49675.

With these servers running, the attacking host can scan the local network to find active hosts and their open ports. Once there is an open port, there will also be a service listening on

this port [5]. The malicious attacker can use the open port information to look for possible vulnerabilities and suitable exploits [1,3,4,6,7].

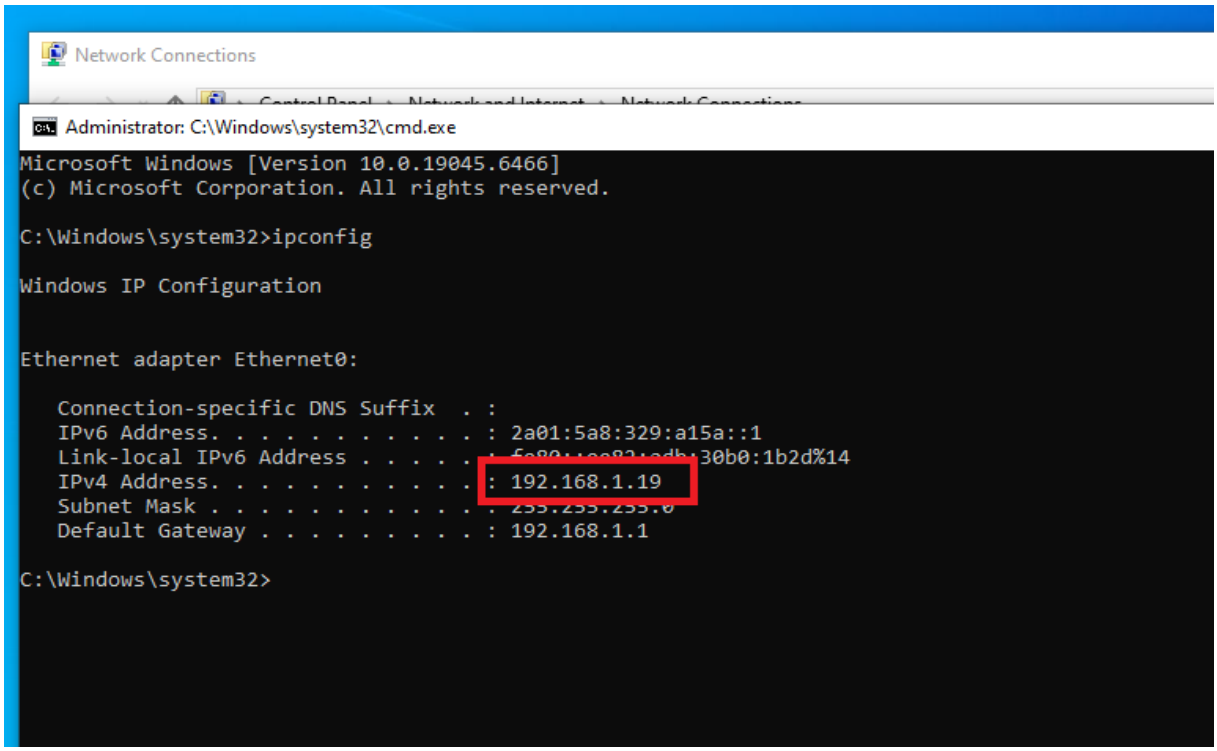


Fig. 1. The IPv4 address of the victim host

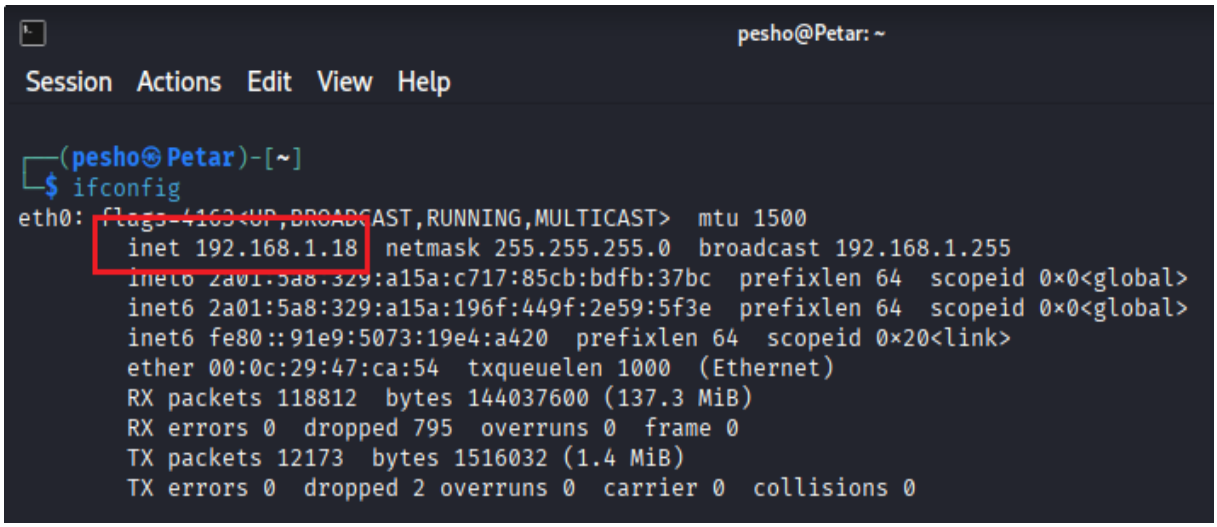


Fig. 2. The IPv4 address of the attacking host

The network scanner that will be used for the research purposes is Naabu version 2.7.0 (fig. 3). The first step is to update Naabu before using it. The first command that will be used for scanning is “sudo naabu -host 192.168.1.19”. Fig. 4 shows that the scan found 10 open ports. Their numbers are 3306,106,80,443,25,21,110,3389,79 and 443.

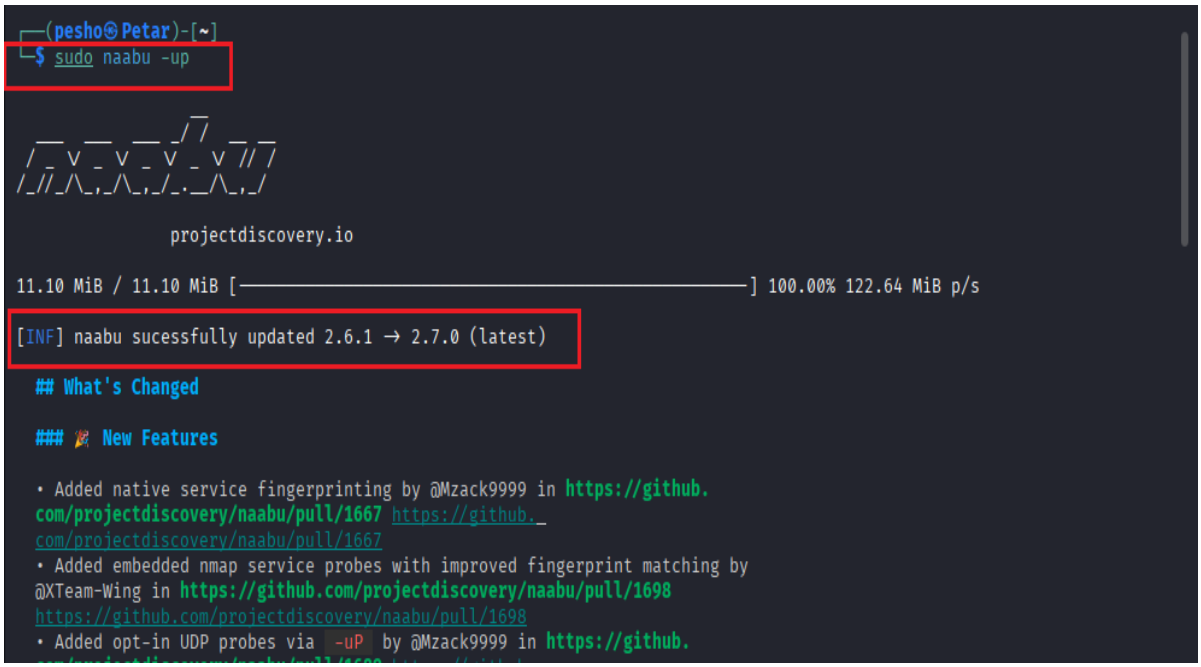


Fig. 3. The successfully updated network tool

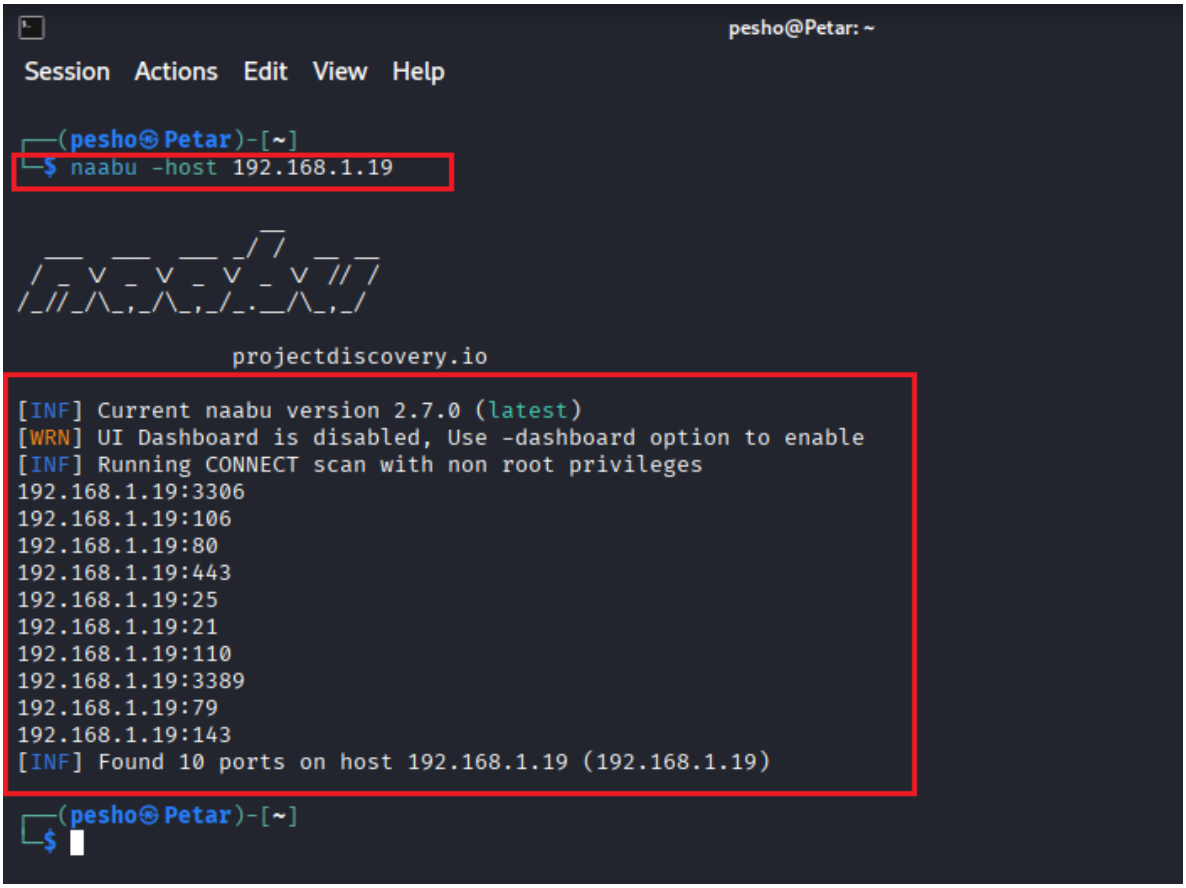


Fig. 4. The found ports after first network scan

With the command "naabu -p 1-65535 -host 192.168.1.19" the attacking host scans all 65535 ports and in this case 13 open ports are found. The additional open ports are 105, 2224, and 7680 (Fig. 5).

The next scan was performed using the command "naabu -host 192.168.1.19 -v -stats -verify". This command displays a detailed information when performing the network scan. It also verifies which ports are open. The scan detected 10 open ports again (fig. 6).

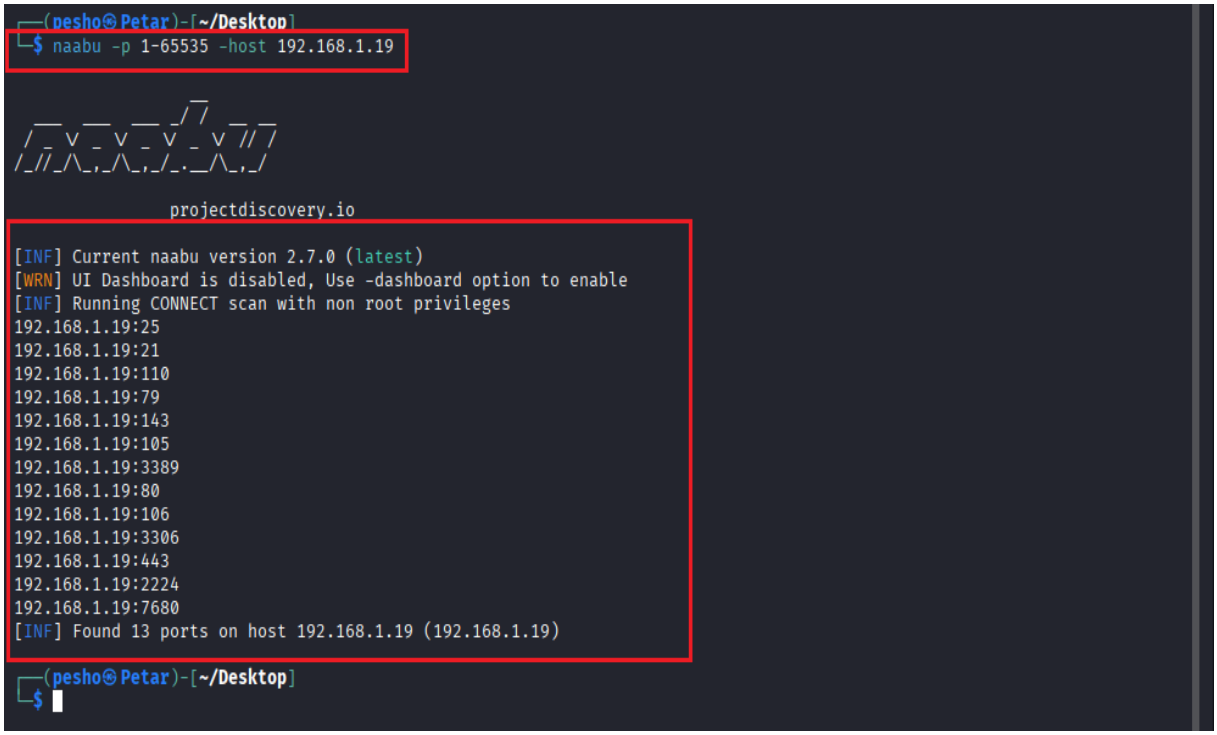


Fig. 5. The network scan with the command "naabu -p 1-65535 -host 192.168.1.19"

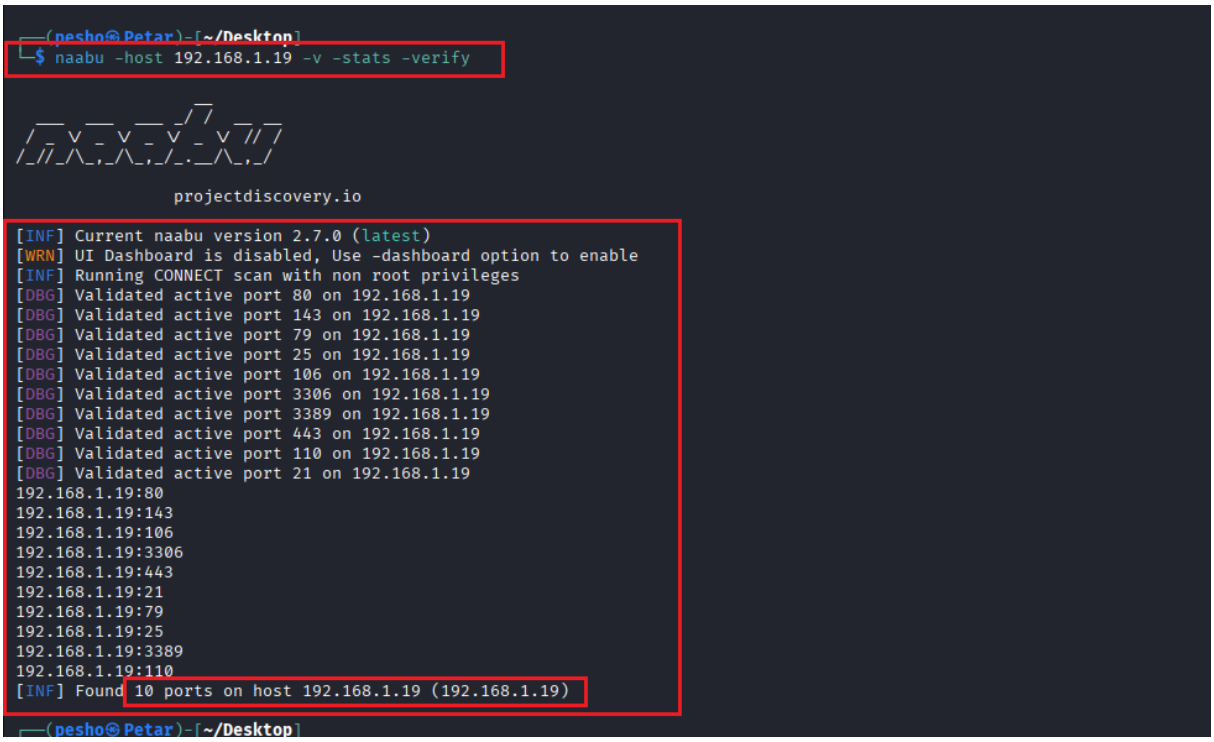


Fig. 6. The network scan with the command "naabu -host 192.168.1.19 -v -stats -verify"

The next scan aims to find active hosts in the controlled local computer network. This scan uses the command "naabu -sn -host 192.168.1.0/24". The scan found 10 active hosts in

the controlled local network 192.168.1.0/24. Naabu finds active hosts in the local network very quickly. This can be useful when investigating a cybersecurity incident (Fig. 7).

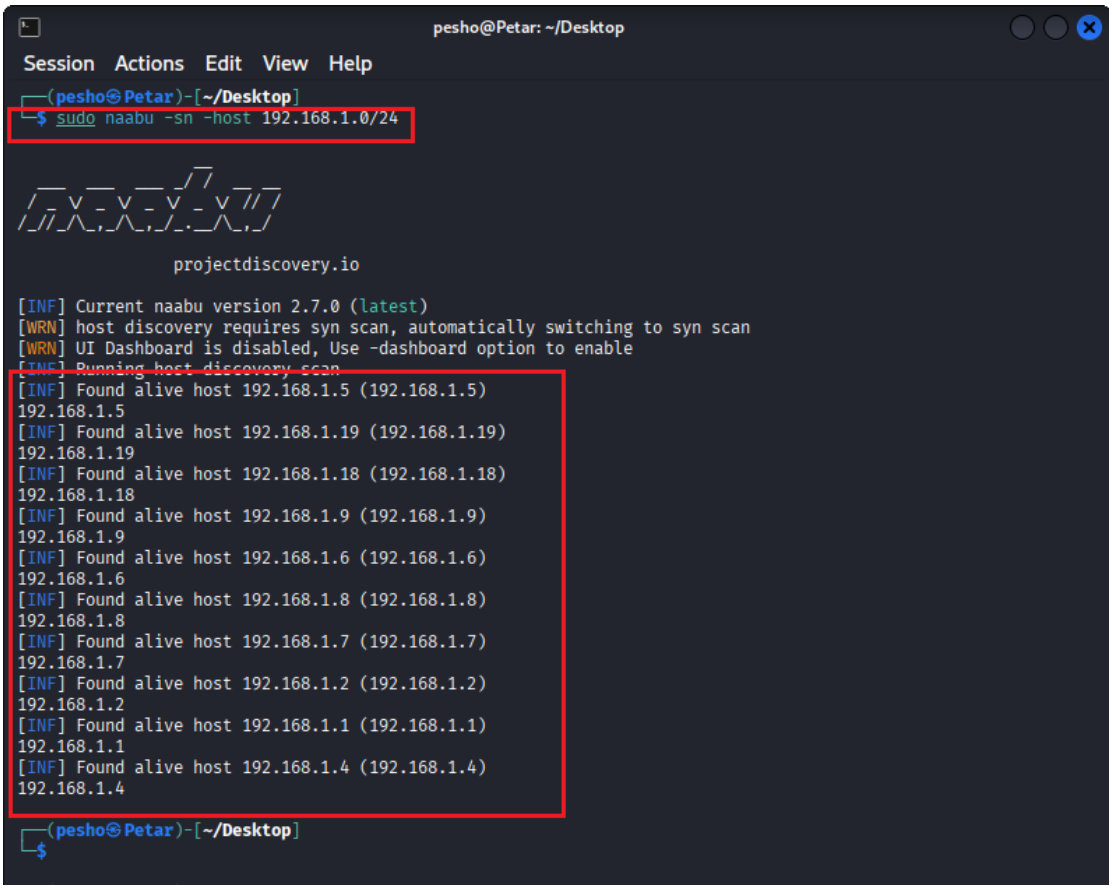


Fig. 7. The network scan with the command "naabu -sn -host 192.168.1.0/24"

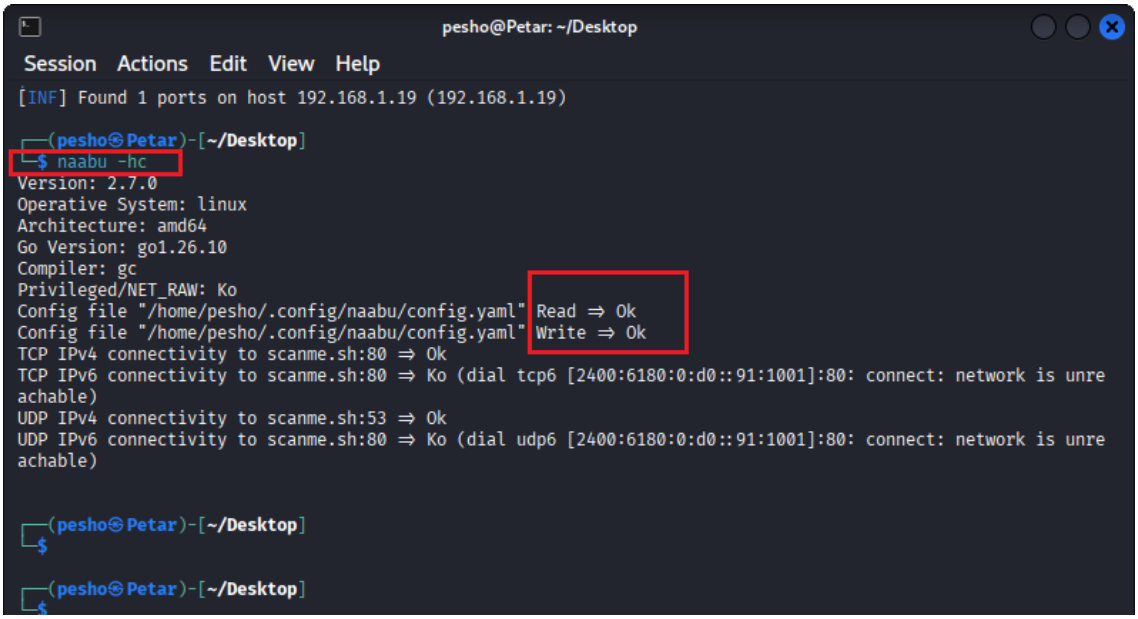


Fig. 8. The results after execution the command “sudo naabu -hc”

Naabu has a diagnostic command, “sudo naabu -hc”, which displays information about the program's configuration. The output of this command in Fig. 8 is shown.

The final command, “naabu -p - -host 192.168.1.19 -v -stats -sD -debug -json”, scans all 65,535 ports on the victim host and displays the results in JSON format. The JSON output can later be imported into a network scanning database for further analysis (Fig. 9).

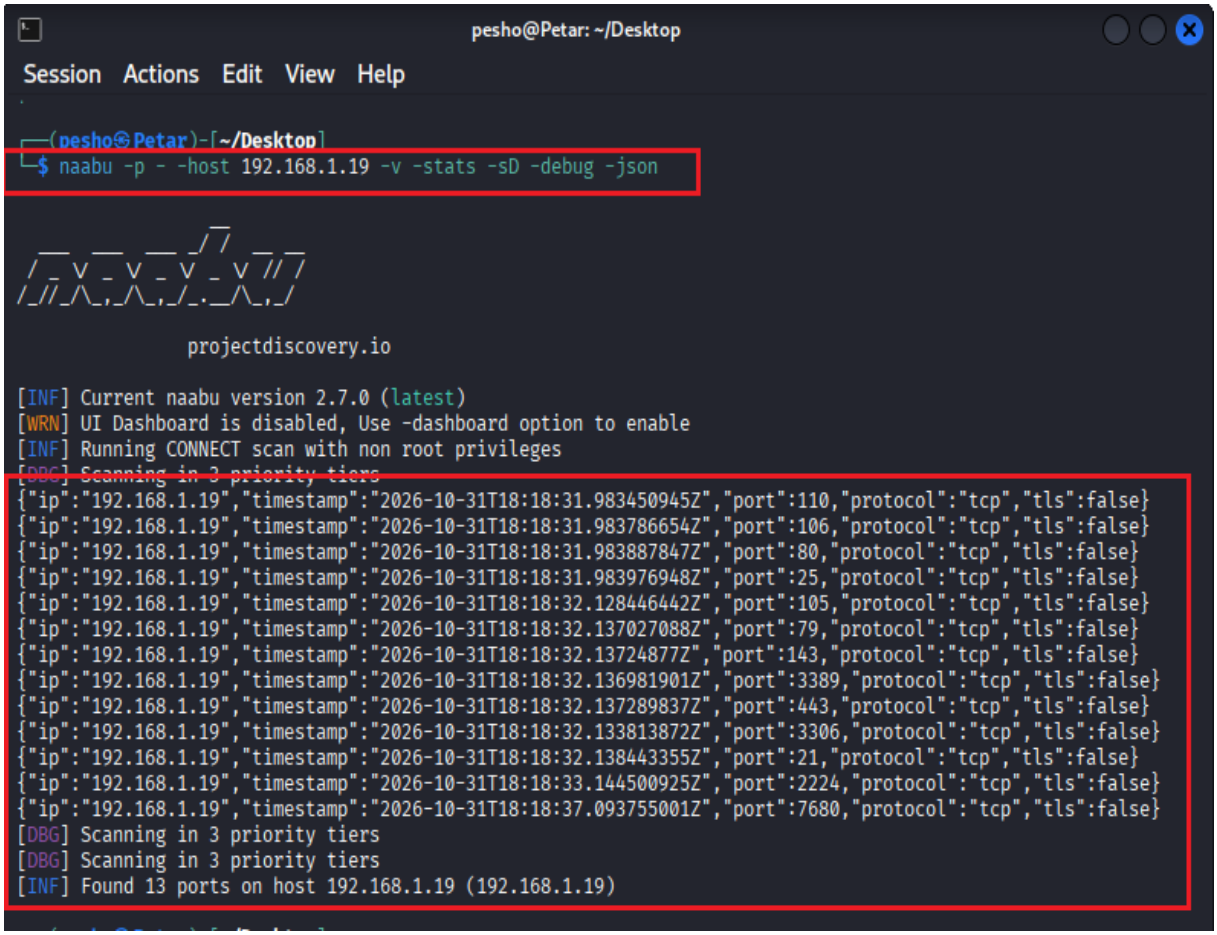


Fig. 9. The achieved results in JSON format

5. Conclusions

Naabu detected active hosts and open ports in the tested controlled local network. Network administrators can use these results to find open ports and possible security risks. The system administrators can use these results to improve network security and prevent unwanted access.

The comparison showed that Naabu is useful for fast and automated port scanning. It is easy to use and can quickly detect open ports even when working with larger computer networks. Nmap is more suitable for detailed scans because it provides information about running services and devices.

Both tools are useful for network security, but they serve different purposes. The choice depends on the type of scan and the information that needs to be collected. Naabu is a good option when open ports need to be found quickly. Nmap is a better choice for detailed network analysis.

References

[1] Agrawal, A. M. K., Bolli, D. B., Teja, C., Budhwani, T. P., Sehgal, L., Dharia, J. N., & Aggarwal, A. (2021). Offensive Web Application Security Framework. Design Engineering (London), ISSN: 0011-9342, Year 2021, Issue: 9, pp. 17334 – 17342.

[2] Annaufal, A. N., Ardhani, M. N., Bintang, S., Simangunsong, G. A., Faylasuf, H. F., Wicaksana, A. D., ... & Mindara, G. P. (2025). Analisis Kerentanan pada Situs Buatinkamu. id dengan Pengujian Penetrasi Metode Black Box. Explore, 15(1), 11-17., p-ISSN : 2087-894X, e-ISSN : 2656-615X.

[3] Fediushyn, O., Khivrenko, H., Popova, N., & Stadnik, V. (2026). Design and implementation of an integrated automated vulnerability scanning platform for web application security assessment, https://doi.org/10.20998/3083-6298.2026.02.11.

[4] Goyal, D., Subramanian, S., Peela, A., & Shetty, N. P. (2024). Hacking, the lazy way: LLM augmented pentesting. arXiv preprint arXiv:2409.09493, https://doi.org/10.48550/arXiv.2409.09493.

[5] Hussain, K., Sheikh, M. A. U., Naing, T., Hussain, M., & Amin, N. U. (2025). Reshaping Cybersecurity Practices by Optimizing Web Application Penetration Testing. In Reshaping CyberSecurity With Generative AI Techniques (pp. 395-410). IGI Global Scientific Publishing, DOI: 10.4018/979-8-3693-5415-5.ch011.

[6] Lavhate, S., Shaikh, S., Bangal, S., Borawake, V., Shinde, K., & Patil, K. (2026, April). Optimizing Bug Bounty Recon Workflows using Automated Asset Discovery and Vulnerability Correlation, 2026 9th International Conference on Inventive Computation Technologies (ICICT), Kirtipur, Nepal, 2026, pp. 1050-1056, doi: 10.1109/ICICT68280.2026.11511063.

[7] Naing, T. (2024). Reshaping Cybersecurity Practices by Optimizing Web Application. Reshaping CyberSecurity With Generative AI Techniques, 395, DOI: 10.4018/979-8-3693-5415-5.

[8] Riskhan, B., Sheikh, M. A. U., Hossain, M. S., Hussain, K., & Hussain, M. (2025). A Methodical Approach to Exploiting Vulnerabilities and Countermeasures Using AI. In Utilizing Generative AI for Cyber Defense Strategies (pp. 287-308). IGI Global Scientific Publishing, DOI: 10.4018/979-8-3693-8944-7.ch008.

[9] Varma, K. R., Sharma, S. S., Kulkarni, Y. Y., & Samdurle, S. S. (2023, December). ReconMaster: A CLI Based Web Reconnaissance Tool. In 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE, https://doi.org/10.1109/ICTBIG59752.2023.10455983.

[10] Wittemeier, H. (2025). Sigma Rule based eBPF Logger for Containerized Environments (Doctoral dissertation, Master's Thesis, Faculty of Information, Media, Electrical Engineering, Institute of Computer, and Communication Technology, Cologne, Germany).

[11] Zhu, H., Luo, W., Tian, Z., Tao, K., Chen, Q., & Xu, F. (2024, October). Focusing on topology map generation and adjustment in power network asset mapping scenarios, 2024 8th International Conference on Electrical, Mechanical and Computer Engineering (ICEMCE), Xi'an, China, 2024, pp. 823-830, doi: 10.1109/ICEMCE64157.2024.10862845.