Network Traffic Analysis Tool Evaluation

Joshua Lopez

California Lutheran University

IT-540

Wayne Snyder

February 5, 2025

Network Traffic Analysis Tool Evaluation

As always, documentation is critical to your analysis in Digital Forensics. It provides a clear, concise, step-by-step view of how evidence was captured. It validates and lends structure and credibility to your investigation. Noting in detail who, what, when, and where the evidence was collected and organizing evidence by time and function are best practices (Easttom, 2021, p. 329). That methodical approach continues in Network Analysis. The network analysis tools I believe would be great additions to DigiFirms lab are NMAP to map out ports and services and TCPDUMP as a network packet analyzer.

NMAP is known in the Information Security industry as one of the most versatile tools for port scanning (Install NMAP: sudo apt-get install). It allows you to verify that a host is active. NMAP can promptly identify devices such as servers, routers, switches, or mobile gadgets across singular or multiple networks. It can also recognize services running on a network along with application / OS version information (Keshav Xplore & Originally published at https://www.keshavxplore.in, 2023).

Scanning is used to identify active devices when mapping a network. For example, running ping scan nmap -sp 192.168.1.1/24 can identify active devices within a specified subnet. You can also do a single-host scan with a domain name or IP Address nmap scanme.nmap.org. This will scan single-host for 1,000 renowned ports. The output shows devices and port services running in their current state(open, filtered(firewall or other network obstacle blocking port), etc.) and names.

NMAP with the -sS option can also perform a stealth scan nmap -sS scanme.nmap.org by sending a SYN packet and analyzing the (SYN/ACK)response. Never completing the 3-way handshake(stealth action), making it difficult for the target to pinpoint the scanning source. The scan can be run with -sV option nmap -sV scanme.nmap.org to obtain the application version. Version and OS operating on a device are valuable information when penetration testing. Knowing the version information, you could look up any associated vulnerabilities. The -sV option will also scan the OS running on a device. One of the advanced features of NMAP is performing an intensive scan with the -A option nmap -A scanme.nmap.org. This is a comprehensive scan for OS, version, script-scanning, and traceroute functionality. Although intensive scans for more detailed information, more probes are retrieving the data, heightening the risk of being detected. Scans can also provide verbose(-v option) output to the console and copy output to a file(-oN option). This is useful to see NMAP's step-by-step actions to acquire the data.

For network packet analysis, I recommend TCPDUMP. Capture and inspect network traffic in real-time. A valuable tool for security professionals who need to understand and investigate network behavior. Focusing on traffic from the eth0 interface**tcpdump -i eth0,** we use the -i option. To view all available network interfaces(-D option), run **tcpdump -D.** TCPDUMP can also retrieve traffic on a specific host or specific port(**tcpdump** host <hostname or IP>, **tcpdump** port <port#>) (Miessler, 2004).

For a more advanced filtering. You can scan by protocol. For example, **tcpdump tcp or tcpdump udp** to pull specific protocol traffic. By source(src option) **tcpdump src host 192.168.1.100.** This will scan all traffic from the specified host. By destination(dst option) **tcpdump dst port 443.** This will scan for traffic with destination to port 443. For a broader perspective, scan for traffic within a network(net option) **tcpdump net 192.168.1.0/24.**

For verbose logging output, there are 3 levels of verbosity. Option -v for verbose, -vv for more verbose, and -vvv for most verbose. This is a valuable option when needing to see all the details of the actions performed by the scan. With such detail, output can be lengthy. With TCPDUMP -w option, you can save the captured traffic to a file **tcpdump -w capture.pcap -i eth0.** To read the capture file, use the -r option **tcpdump -r capture.pcap.** Another valuable option is to capture TCP flag traffic. For example, you may want to scan for RST(**tcpdump 'tcp[tcpflags] & tcp-rst != 0'**), SYN(**tcpdump 'tcp[tcpflags] & tcp-syn != 0'**), ACK(**tcpdump 'tcp[tcpflags] & tcp-ack != 0'**), or all TCP flag traffic(**tcpdump 'tcp[tcpflags] = 0x01'**) on the network. This would be useful in analyzing the network traffic for activity resembling a possible syn-flood attack.

So far, we have seen quite a bit of these tools' functionality. TCPDUMPS network analysis/debugging can be opened in the Wireshark application for viewing within a GUI. Further, Wireshark offers many methods for reviewing packet-trace dumps, such as statistical analysis, graphs, filtering to drill down to specific traffic, and more. TCPDUMP is compatible with unix-like OS like Linux, MacOS, and Windows versions of TCPDUMP called WinDump (Tcpdump, 2025). NMAP’s host discovery, port scanning, service, and devices are just some of the tool's valuable functionalities. NMAP offers a command line application, Zenmap GUI, and is compatible with Windows, MacOS, and Linux (Nmap, 2024). The compatibility and valuable functions of the command line and GUI make these strong tools for organizations to have in their arsenal.

References

Easttom, C. (2021). Digital forensics, investigation, and response (4th ed.). Jones & Bartlett Learning.

Keshav Xplore & Originally published at https://www.keshavxplore.in. (2023, October 18). What is Nmap and How to Use it in Cybersecurity | Ethical Hacking. Medium. Retrieved February 1, 2025, from <https://medium.com/@keshavxplore/what-is-nmap-and-how-to-use-it-in-cybersecurity-ethical-hacking-878cfbb64550>

Miessler, D. (2004, January 4). A tcpdump Tutorial with Examples [Blog]. danielmiessler. Retrieved February 1, 2025, from <https://danielmiessler.com/blog/tcpdump>

Nmap [Wiki]. (2024, December 27). Wikipedia. Retrieved February 2, 2025, from <https://en.wikipedia.org/wiki/Nmap>

tcpdump [Wiki]. (2025, January 19). Wikipedia. Retrieved February 2, 2025, from <https://en.wikipedia.org/wiki/Tcpdump#:~:text=Tcpdump%20works%20on%20most%20Unix,the%20Windows%20version%20of%20libpcap.>