Common Tools for System Analysis in Cyber Security

Olivia Criscione

CYBR 306

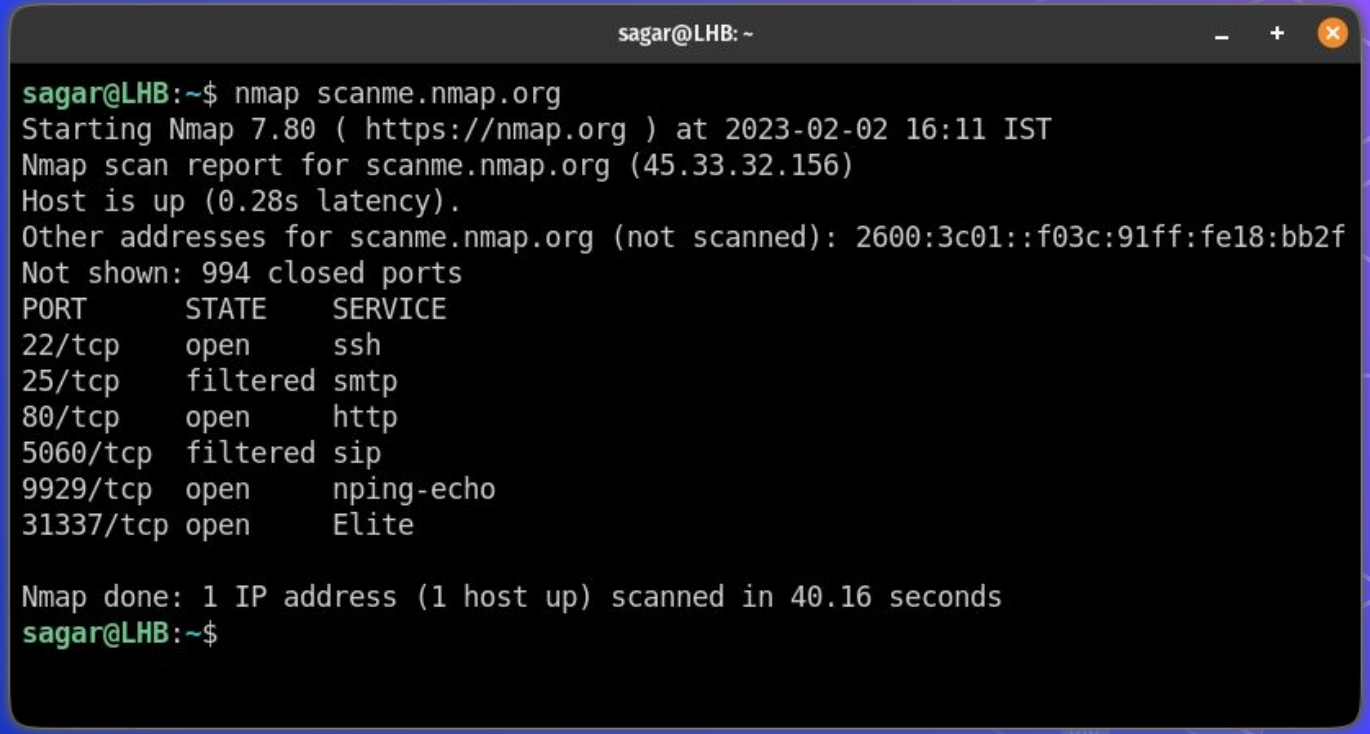
Tool 1 - Nmap

Source: https://nmap.org/

- Nmap (Network Mapper), is an open-source (free) network scanning tool designed for host discovery and service identification.
  - Nmap aids in identifying open ports, services running, and potential vulnerabilities by using IP packets to scan large networks.
  - One pro of Nmap is that it offers flexibility, is actively maintained, and supports scripting for advanced functionality in security.
  - One con of Nmap is that it is hard to pick up without having extensive knowledge about network engineering. Nmap scans can also be blocked due to heavy traffic flow being created.
  - Nmap enhances network visibility for companies by facilitating proactive vulnerability management and strengthening overall security.

What does Nmap look like in use?

This is an example of nmap searching for open ports in a system



https://linuxhandbook.com/nmap-command/

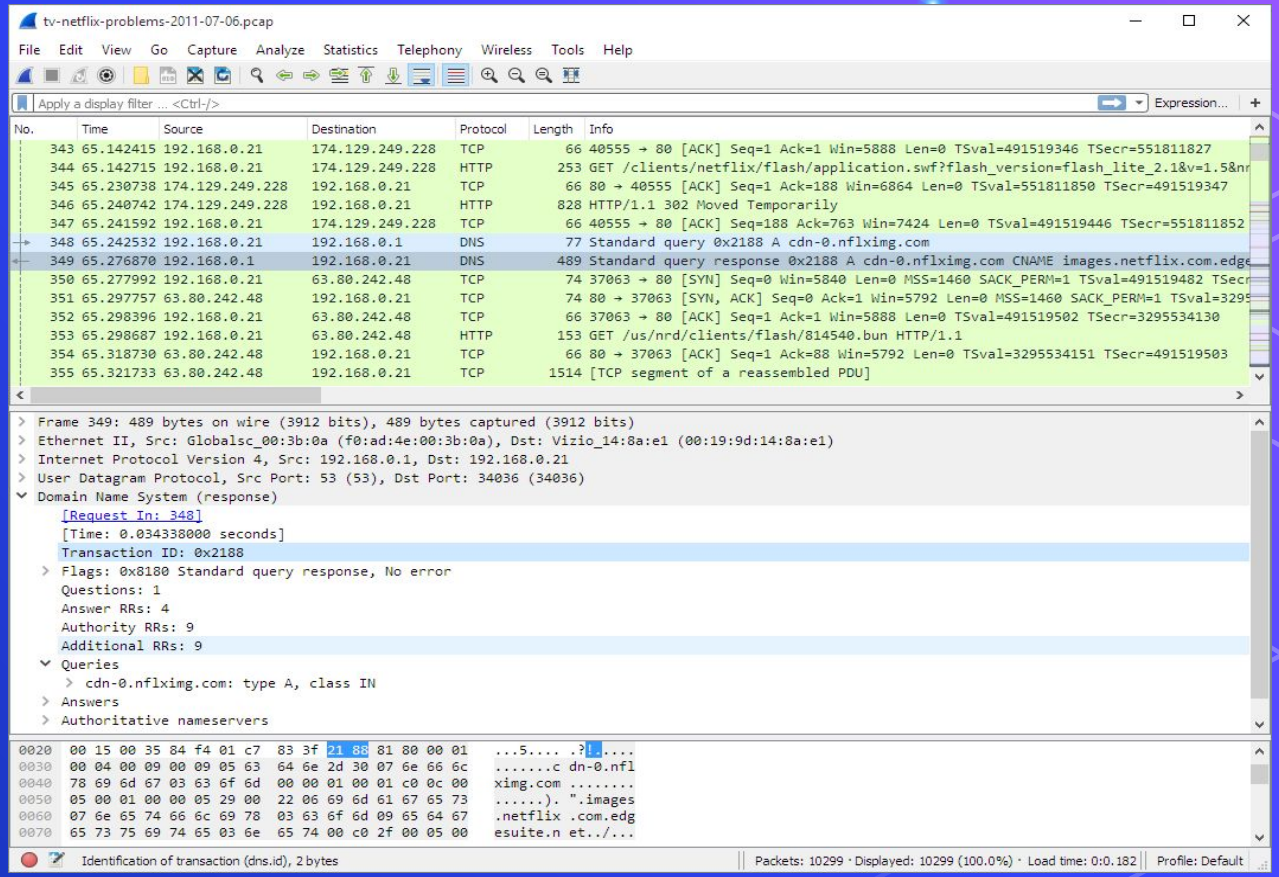
Tool 2 - Wireshark

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

- Wireshark is another widely-used open-source packet analyzer, that allows users to capture, analyze current network traffic, and troubleshoot networks.
  - Enables an in-depth analysis of network packets, aiding in the detection of suspicious activities and possible security threats.
  - A pro of wireshark is the powerful packet analysis capabilities provided that support various protocols and support.
  - One con of wireshark is that using it in an efficient way requires an extensive understanding of networks so it is best utilized by network engineers. Is harder to pick up without prior knowledge on network security and configuration.
  - Wireshark strengthens companies network security by providing insights into ongoing activities and threats.

What does Wireshark look like in use?

This is an example of the GUI of wireshark. This is what the main wireshark window looks like after loading a few packets



https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html

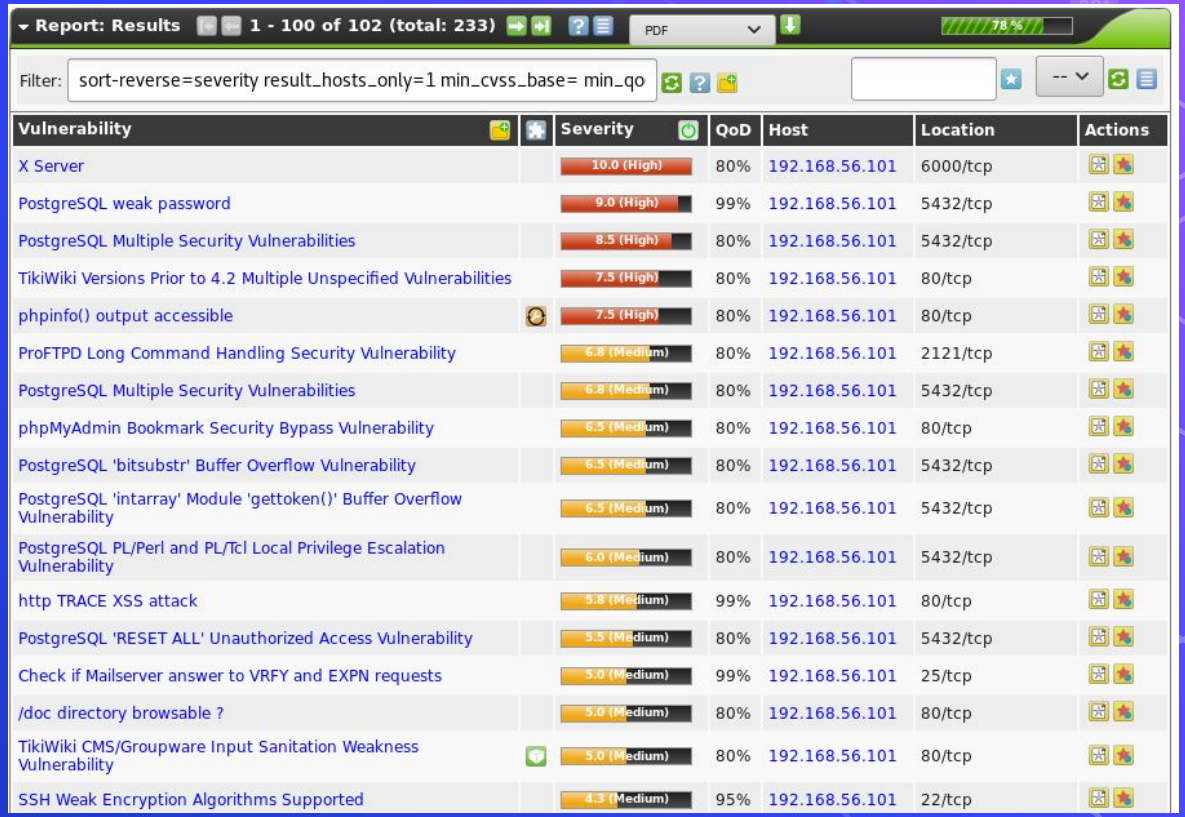
Tool 3 - OpenVAS

- OpenVAS (Open Vulnerability Assessment System), is an open-source network security vulnerability scanning and management tool provided by Greenbone.
  - OpenVAS identifies vulnerabilities in systems, applications, and networks, assisting companies in securing their digital assets from security threats.
  - One pro of OpenVAS is that it is fast, easy to use, and is updated on a daily basis.
  - One con is that you need a virtual machine player in order to use OpenVAS. You also can only do so much with the free version.
  - Using OpenVAS enhances companies overall security by systematically identifying and addressing potential vulnerabilities.

https://resources.infosecinstitute.com/topics/pen-testing/a-brief-introduction-to-the-openvas-vulnerability-scanner/

What does OpenVAS look like in use?

This is an example of the results of an OpenVAS network security scan.



https://www.rapid7.com/blog/post/2016/11/22/how-to-use-openvas-to-audit-the-security-of-your-network-22/

Tools

- Consistent updates and patching of cybersecurity tools are essential to addressing known vulnerabilities and ensure that companies are well-prepared against potential cyber threats.
- The integration of cybersecurity tools creates a comprehensive defense strategy, enhancing overall cybersecurity protection for organizations.
- Reduces the overall security vulnerabilities which in turn creates trust within organizations.
- Tools like Nmap, Wireshark, and OpenVAS contribute to real-time monitoring which allows security teams to identify and respond to potential security incidents in a timely manner.
- It is important to have experts interpret the results of scans to identify how to respond to the results.

Conclusion

- Cybersecurity technologies are essential for incident response since they help quickly detect and contain security issues in addition to helping to discover vulnerabilities.
- Tools like Wireshark and Nmap contribute to continuous security monitoring, allowing organizations to adapt and respond swiftly to security vulnerabilities.
- Cybersecurity tools assist organizations in maintaining regulatory security compliance and updates by providing an efficient way to monitor and report security measures.
- Human interaction is needed for all three of these tools in order to adequately understand and respond to the results that these tools provide.