For vulnerability scanning, we will be using popular tools. All are powerful tools that can identify potential security flaws in a network or system.

Nmap:

1. Nmap is a popular network mapping and vulnerability scanning tool. It is used to identify open ports, services, and vulnerabilities on a network. Nmap can be used to scan both internal and external networks. It supports a wide range of scanning techniques, such as ping scans, TCP scans, UDP scans, and OS detection. Nmap is a command-line tool and provides a GUI interface called Zenmap.

To use Nmap, you can simply enter the target IP address or hostname in the command-line interface followed by the desired scan type. For example, to perform a TCP scan on a target, you can run the following commands:
nmap -sS <target_ip_address>

map -sS <target_ip_address>

Nmap also provides various configuration options and settings to customize the scan, such as timing options, output formats, and script options.
Pros:

- Supports a wide range of scanning techniques
- Provides a GUI interface for easier use
- Offers extensive customization options and settings
- Highly effective for network mapping and vulnerability scanning

Cons:

- Can be slow when scanning large networks
- Requires some level of expertise to use effectively

Nikto:

2. Nikto is a web server vulnerability scanner that can detect a wide range of vulnerabilities on web servers. It checks for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and directory traversal. Nikto is a command-line tool and provides a simple interface for scanning web servers.

To use Nikto, you can enter the target URL or IP address in the command-line interface followed by any desired options. For example, to scan a web server, you can run the following command:
nikto -h <target_url>

kto -h <target_url>

Nikto also provides various configuration options and settings to customize the scan, such as output formats and SSL options.
Pros:

- Highly effective for web server vulnerability scanning
- Simple and easy to use interface
- Supports multiple output formats
- Provides comprehensive vulnerability reporting

Cons:

- May generate false positives
- Does not detect all types of vulnerabilities

Fierce:

3. Fierce is a domain reconnaissance tool that is used to map out a network and identify vulnerable services. It uses various techniques such as DNS brute forcing and zone transfers to gather information about a domain. Fierce is a command-line tool and provides an interface for scanning domains.

To use Fierce, you can enter the target domain in the command-line interface followed by any desired options. For example, to scan a domain, you can run the following command:
fierce -dns <target_domain>fierce -dns <target_domain>
Fierce also provides various configuration options and settings to customize the scan, such as output formats and verbosity levels.

Pros:

- Highly effective for domain reconnaissance
- Provides comprehensive reporting on domain information
- Customizable and configurable

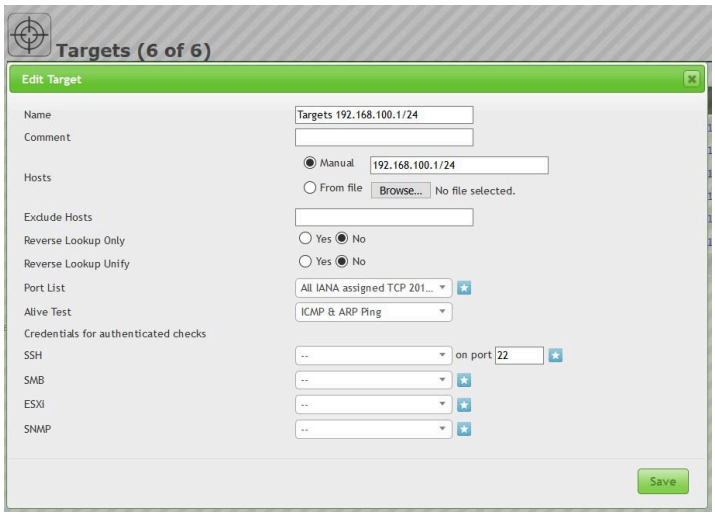
Cons:

- May generate false positives
- Limited to domain reconnaissance and cannot scan for vulnerabilities directly

OpenVAS:

4. OpenVAS is an open-source vulnerability scanner that is used to identify vulnerabilities on a network. It can scan both internal and external networks and provides detailed reports on identified vulnerabilities. OpenVAS is a command-line tool and provides a web interface for managing and viewing scans.

To use OpenVAS, you can enter the target IP address or hostname in the web interface and select the desired scan type. OpenVAS provides a wide range of scanning options, such as vulnerability scans and compliance scans.



Pros:

- Highly effective for vulnerability scanning
- Supports a wide range of scan types
- Provides detailed reporting on identified vulnerabilities
- Offers a web interface for easier management

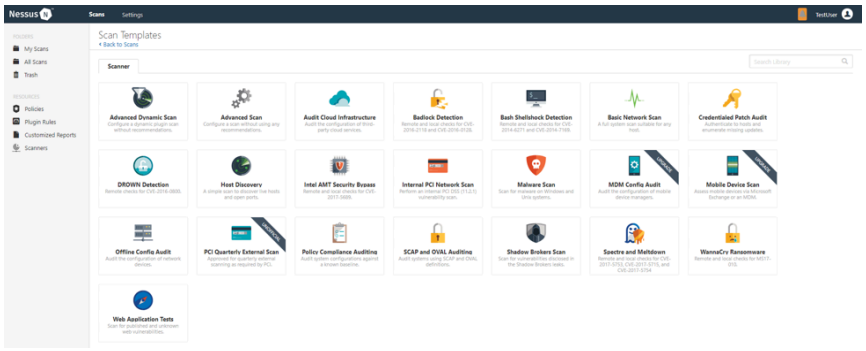
Cons:

- Can be resource-intensive, meaning that it may require a significant amount of system resources (such as CPU and memory) to run scans. This can potentially impact the performance of the system on which it is running, particularly if the system is already under heavy load. Therefore, it's important to ensure that the system has sufficient resources to support OpenVAS scans and to adjust its configuration settings appropriately to minimize any impact on system performance.

Nessus:

5. Nessus is a proprietary vulnerability scanning tool that allows us to scan networks and systems for vulnerabilities. It has a large database of over 100,000 plugins that can detect vulnerabilities in operating systems, applications, and databases. The tool also allows us to configure and customize scans, generate reports, and manage vulnerabilities.

To use Nessus, we need to first download and install it on our system. We can then access the tool through the Nessus web interface. We can set up scans by defining targets, configuring scan options, and scheduling scans. We can also view scan results and generate reports.



Pros of Nessus:

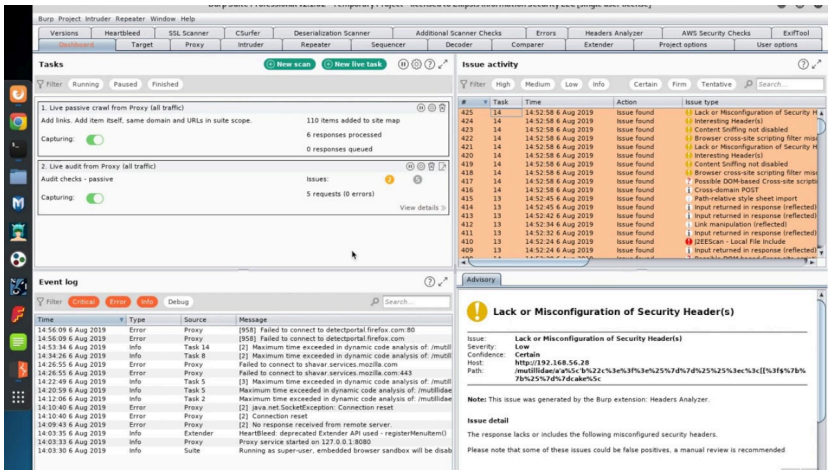
- Nessus has a larger database of plugins than OpenVAS, making it effective at detecting vulnerabilities.
- It allows us to configure and customize scans, generate reports, and manage vulnerabilities.
- It has a user-friendly web interface.

Cons of Nessus:

- Nessus is a proprietary tool and is not freely available.
- It can be expensive to use, especially for large-scale scans.
- It may generate false positives or false negatives in some cases.

BurpSuite:

6. BurpSuite is a Java-based platform used for testing web applications. It is widely used by penetration testers and web developers as a comprehensive tool for performing various web application security tests. BurpSuite is available in both free and paid versions. The free version, known as BurpSuite Community Edition, offers limited features, while the paid version, BurpSuite Professional, offers advanced features such as automated scanning, session handling, and more.
How it works:
BurpSuite can be used to intercept and manipulate HTTP/S traffic between a web browser and a web server. It can perform various security tests such as web vulnerability scanning, SQL injection, cross-site scripting, and more. It offers multiple scanning techniques and options, including active and passive scanning modes, to test the web application's security vulnerabilities.
Configuration options and settings:
BurpSuite offers various configuration options and settings to customize the security scans. The tool has a user-friendly interface that allows users to configure and customize the scans according to their needs. Users can define the scope of the scan, set up authentication, configure proxy settings, and more.



Pros:

- BurpSuite is a comprehensive tool that offers multiple scanning techniques to test web application vulnerabilities.
- It has a user-friendly interface that allows users to configure and customize the scans according to their needs.
- The paid version offers advanced features such as automated scanning, session handling, and more.
- It offers comprehensive documentation and support.

Cons:

- The free version offers limited features compared to the paid version.
- BurpSuite can be resource-intensive, requiring a powerful system to perform large-scale scans.

- The tool requires some technical expertise to use effectively.
- The paid version is expensive.

Citations:

Unknown. (n.d.). BURP scanner - web vulnerability scanner from Portswigger. Burp Scanner - Web Vulnerability Scanner from PortSwigger. Retrieved February 21, 2023, from https://portswigger.net/burp/vulnerability-scanner
Unknown. (2021, August 13). Nessus Reviews & Ratings 2023. TrustRadius. Retrieved February 21, 2023, from https://www.trustradius.com/products/nessus/reviews?qs=pros-and-cons#reviews
Unknown. (n.d.). Greenbone openvas. OpenVAS. Retrieved February 27, 2023, from https://www.openvas.org/
GeeksforGeeks. (2022, September 8). Fierce - DNS reconnaissance tool for locating non-contiguous IP Space. GeeksforGeeks. Retrieved February 27, 2023, from https://www.geeksforgeeks.org/fierce-dns-reconnaissance-tool-for-locating-non-contiguous-ip-space/
Cirt.net. Nikto2 | CIRT.net. (n.d.). Retrieved February 21, 2023, from https://cirt.net/Nikto2
II, J. B. (2022, May 19). What is Nmap and why do you need it on your network? Network World. Retrieved February 27, 2023, from https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html