**Identify Targets and Run Scans**

**By: Long Trang**

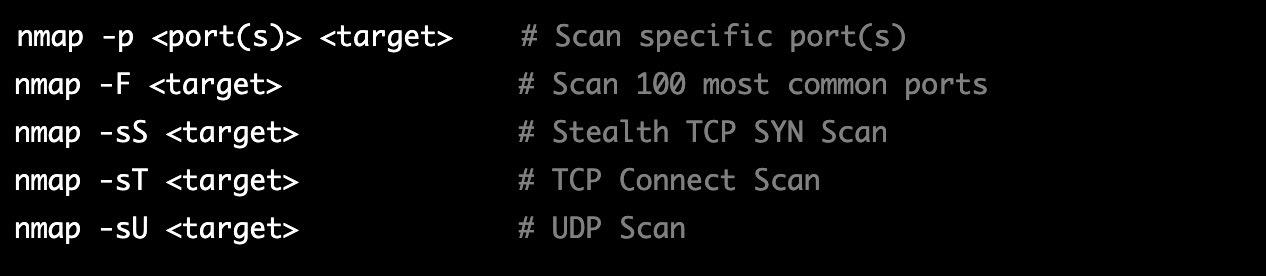
**Tool: Nmap**

**Purpose:** Nmap (Network Mapper) is a powerful open-source tool used for network exploration, management, and security auditing. It is primarily used to scan networks, identify hosts, and discover open ports and services running on them. a versatile tool that can be used for a variety of purposes, such as network inventory, vulnerability scanning, and penetration testing. It can provide valuable information about the network topology, identify potential security weaknesses, and help system administrators to secure their network infrastructure.

**Banner Grabbing:**



**Port Scanning:**



Limitation:

* Nmap can sometimes generate false positives, which can be misleading and waste time and resources.
* Firewalls can limit the accuracy of Nmap scans, as they can block or limit the scan traffic, leading to inaccurate results.
* Some targets may not respond to Nmap scans, making it difficult to identify open ports, services, and operating systems.

**Tool: OpenVAS**

**Purpose:** OpenVAS (Open Vulnerability Assessment System) is a free and open-source vulnerability scanner used for identifying security vulnerabilities in computer systems and networks. It consists of several components, including a scanner, a server, and a collection of plugins for vulnerability testing. Designed to detect vulnerabilities in various systems, including servers, desktops, web applications, and other networked devices. It works by performing scans of the target system or network, identifying vulnerabilities and generating reports that can be used to remediate the security issues.

**Command for Scans:**

sudo omp -u <username> -w <password> --xml="<create\_target><name><Artemis></name><hosts><TARGET\_IP\_OR\_DOMAIN></hosts></create\_target>"

**Limitations:**

* OpenVAS scans can consume significant amounts of network bandwidth, especially if they are performed on large networks or systems. This can cause performance issues on the target system or network, and may also impact other network operations.
* can be resource-intensive, especially when running large or complex scans. It can consume significant amounts of CPU and memory resources, which may cause performance issues on the scanning system.
* can be complex to set up and configure, especially for users who are not familiar with vulnerability scanning tools. It requires expertise in network security and vulnerability management to use effectively.

**Tool: Metasploit**

**Purpose:** Metasploit is an open-source penetration testing framework that allows security professionals and hackers to test the security of computer systems and networks. Its purpose is to help users identify vulnerabilities in target systems and exploit them to gain access to the system, and ultimately, to provide insight into potential security risks and to help organizations better protect themselves against cyber attacks.

**Command Line:**

* db\_nmap: This command is used to store the results of a network scan performed with the Nmap tool into the Metasploit database. This allows you to use the information gathered during the scan to perform further actions such as vulnerability scans, exploit attempts, or other attacks against the target.
* search: This command is used to search for specific exploits, payloads, or auxiliary modules within the Metasploit framework. It can be used with various filters to narrow down the search results based on the type of module, operating system, or vulnerability being targeted.

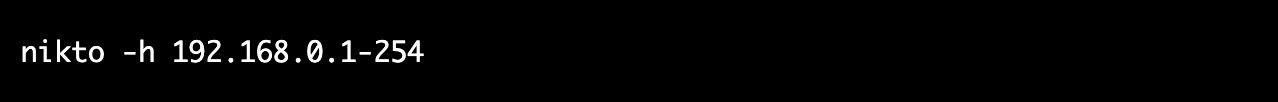
**Limitations:**

* Modern security systems such as intrusion detection and prevention systems, firewalls, and antivirus software can detect and block many of the exploits that Metasploit uses. This can limit the effectiveness of the tool against well-defended systems.
* has a steep learning curve and a complex user interface, which can make it difficult for new users to get started. It may require a significant amount of time and effort to master the tool and use it effectively.

**Tool: Nikto**

**Purpose:** Nikto is an open-source web server scanner that is designed to identify potential vulnerabilities and security weaknesses in web servers and web applications. The tool uses a comprehensive database of known vulnerabilities and attack signatures to test web servers and identify any known security issues.

Scan a range of IP addresses:



Scan a list of hostnames:



**Limitations:**

* Nikto is primarily designed for scanning web servers and web applications, and may not be effective for other types of network devices or systems.
* While Nikto provides a range of scanning options and plugins, it may not always be possible to customize the tool to meet the specific needs of a given security testing scenario.
* Depending on the size and complexity of the target network or application, Nikto scans can take a long time to complete, potentially impacting system performance and availability. This can make it difficult to use the tool in certain situations or on large-scale networks.

**Tool: WireShark**

**Purpose:** Wireshark is a network protocol analyzer that allows for the real-time examination and analysis of network traffic by capturing and dissecting data packets. It provides detailed insights into network performance and can be used to identify potential vulnerabilities by reviewing connection-level information and the contents of data packets. In summary, Wireshark is a powerful tool for monitoring and analyzing network traffic, offering the ability to assess network activity and identify security concerns in real-time.

**Techniques:**

* ARP scanning: ARP is a protocol used to map a network address (such as an IP address) to a physical address (such as a MAC address). By sending an ARP request to a network, it is possible to discover which hosts are present on the network. To perform ARP scanning with Wireshark, filter for ARP packets using the filter "arp".
* DHCP scanning: The Dynamic Host Configuration Protocol (DHCP) is a protocol used to assign IP addresses to devices on a network. By monitoring DHCP traffic, it is possible to discover which hosts have been assigned IP addresses by the DHCP server. To perform DHCP scanning with Wireshark, filter for DHCP packets using the filter "bootp".

**Limitations:**

* Wireshark cannot decrypt encrypted network traffic, so if the target network uses encryption (such as HTTPS), it may be difficult or impossible to capture and analyze the data.
* If the network being scanned is heavily congested, it may be difficult to capture all of the traffic or to identify specific hosts or services. In some cases, the sheer volume of traffic may overwhelm Wireshark or the computer running Wireshark.

**Tool: Lynis**

**Purpose:** Lynis is a popular open-source security auditing tool for Unix/Linux systems that is used to perform system hardening and security assessments. It is a command-line tool that scans the system for security vulnerabilities, misconfigurations, and best practices. Lynis can be used to audit a wide range of systems, including servers, workstations, and virtual machines. To help system administrators and security professionals to identify potential security risks and weaknesses in their systems, and to provide recommendations and remediation steps to improve the overall security posture of the system. It can be used to perform regular security audits, compliance audits (such as for HIPAA, PCI DSS, or GDPR), or as part of a vulnerability management program.

**Techniques:**

* Remote system enumeration: Lynis includes a remote system enumeration module that can be used to gather information about a remote system, such as its hostname, IP address, operating system, and kernel version. This information can be used to identify potential vulnerabilities and to determine the best course of action for securing the system.
* Network Scanning:
* 