CYBRARY

Creator: @netshark - Anderson Rodrigues

Nmap
Glossary Terms

1. Firewall - is a hardware or software-based (most common) security solution that, based on a set of rules or instructions, analyzes network traffic to determine which data transmission or reception operations can be performed.

2. IDS - An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm-filtering techniques to distinguish malicious activity from false alarms.

3. Script - A scripting language is a programming language that supports scripts, programs written for a special runtime system that automates the execution of tasks that could alternatively be executed one at a time by a human operator

4. Evasion - In network security, evasion is bypassing an information security device in order to deliver an exploit, attack, or other form of malware to a target network or system, without detection. Evasions are typically used to counter network-based intrusion detection and prevention systems (IPS, IDS) but can also be used to by-pass firewalls and defeat malware analysis. A further target of evasions can be to crash a network security device, rendering it in effective to subsequent targeted attacks.

5. Spoofing - is a type of technological forgery that seeks to deceive a network or a person by making them believe that the source of an information is reliable when the reality is quite different.

6. Sniffer - A Sniffer (or Packet Analyzer / Packet Sniffer) is an application that monitors (sniffs) breach, ports, faults, etc ... in a system, usually used to monitor network traffic and ports, detecting problems and thus improving the system.

7. Pentest - also translated as "penetration test," is a method that evaluates the security of a computer system or network, simulating an attack from a malicious source. The process involves an analysis of the system activities, which involves the search for some potential vulnerability that may be the result of poor system configuration, unknown hardware / software failures, operating system deficiencies or countermeasure techniques. All analyzes submitted by the chosen tests are presented in the system, together with an evaluation of their impact and often with a proposed resolution or a technical solution.

8. Network services - Basically, these tools load in the background, and provide functionality for internal and external network. Some of these well-known services are Apache (http server), Samba (file server), and Squid

9. Security Audit - Its mission is to evaluate the security of a company's information systems. Its purpose, therefore, is to detect flaws and vulnerabilities that could compromise data protection. Thus, if any breach is found, the company can update processes and infrastructures to protect the information.

10. Nmap - ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators, find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

11. Zenmap - Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application, which aims to make Nmap easy for beginners to use while providing advanced, features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

12. NSE - Nmap Scripting Engine is a powerful, versatile and flexible Nmap feature that allows its users to develop and share simple scripts and integrate them with traditional Nmap scans to automate various tasks. Users can only use the scripts made available with Nmap, modify existing scripts, or even develop their own custom scripts that meet their needs.

13. Port Scan - It is the process of sending carefully crafted messages or packages to a target computer with the intention of learning more about it. These probes are usually associated with well-known port numbers or less than or equal to 1024. By carefully applying this technique, you can learn about the services that a system offers to the network as a whole.

14. Network Scan - This scan is designed to locate active hosts on a network (running). This type of scan will identify the systems that can be attacked later or those that can be scanned a little more closely. Scans that fall into this category are those like ping sweeps, which quickly sweep a range of IPs and determine whether an address has a connected host connected to it or not.

15. Vulnerability Scan - This is used to identify weaknesses or vulnerabilities in a target system. This type of scanning is commonly done as a proactive measure to detect problems internally before an attacker can locate these vulnerabilities and act on them. A typical vulnerability scan will discover hosts, access points and open ports, analyze service response, classify threats, and generate reports.

16. Host discovery - Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.

17. Version detection - Interrogating network services on remote devices to determine application name and version number.

18. OS detection - Determining the operating system and hardware characteristics of network devices.

19. Target Specification - Everything on the Nmap command-line that isn't an option (or option argument) is treated as a target host specification. The simplest case is to specify a target IP address or hostname for scanning.
When a hostname is given as a target, it is resolved via the Domain Name System (DNS) to determine the IP address to scan. If the name resolves to more than one IP address, only the first one will be scanned. To make Nmap scan all the resolved addresses instead of only the first one, use the --resolve-all option.

20. IP spoofing - IP spoofing is an attack that consists of masking (spoof) IP packets using addresses of spoofed senders.