Scanning, Enumeration and Vulnerabilities Glossary

Creator: Ajibowu Abiola Sherif (TA)

1. **CIDR** - Classless Inter-Domain Routing - this is used for allowing more flexible allocation of IP addresses than was possible with the original system of IP address classes. It is sometimes called supernetting.[1]
2. **Banners** - these are text-based welcome screens from remote host that displays system information.
3. **Banner grabbing** - this is used for retrieving information about a computer system on a network and capture banners of open ports. It can be performed using Telnet, Netcat or Nmap.
4. **DIG** - Domain Information Groper - this helps network administrators to troubleshoot network related issues. It is used for performing zone transfers.
5. **DNS Records**: DNS servers create a DNS record to provide important information about a domain or hostname, particularly its current IP address.[2]
6. **DVWA** - Damn Vulnerable Web App - this is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a classroom environment.[3]
7. **Enumeration** - the process of enumeration or finding finds what services are running, versions, open shares, account details, or possible points of entry.[4]
8. **Filtered Port** - filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.[5]
9. **FIN Flag** - FIN flag indicates the end of data transmission to finish a TCP connection.[6]
10. **Finger Command** - finger command is used in Unix / Linux to retrieve information about the system users in the network.
11. **Firewall -** This is a piece of computer software intended to prevent unauthorized access to system software or data.
12. **Firewall Rules** - These define what kind of Internet traffic is allowed or blocked.
13. **Hping3** - Hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP

echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.[7]

14. **IDS** - Intrusion Detection System - is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.[8]
15. **Kali Linux** -this is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.[9]
16. **Loopback Interface** - This interface is used by a system to communicate with itself.
17. **Netcat -** This is a computer networking utility for reading and writing from and to network connections using TCP or UDP. It can be used for port scanning, transferring files and port listening.[10]
18. **Network scanner** - A network scanner is a port scanner used to find open ports on multiple devices on the network.
19. **NMAP** – 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.[11]
20. **Open Ports** – Open means that an application on the target machine is listening for connections/packets on that port.
21. **OS Fingerprinting** – This is the process of determining the operating system used by a host on a network.

    - Active Fingerprinting : Active fingerprinting is the process of transmitting packets to a remote host and analysing corresponding replies.It is the most reliable and accurate but cannot be used in highly secured or firewalled environments as it may trigger alerts.

    - Passive Fingerprinting : Passive fingerprinting is the process of analysing packets from a host on a network. The logic behind passive reconnaissance is to capture a packet by sniffing and analysing the same for difference in attribute. The analysis details are compared against a database to identify the OS that sent the packet.[12]
22. **Packet Filtering -** is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.[13]

23. **Packet Loss** - occurs when one or more packets of data travelling across a computer network fail to reach their destination. It is either caused by errors in data transmission, typically across wireless networks, or network congestion.[14]
24. **Penetration Testing** - A test by an outsider that attempts to actually exploit any weaknesses in systems that are vulnerable.
25. **Ping Sweep (ICMP Scan) -** Ping sweep is used to identify the live host from a range of IP addresses by sending the ICMP ECHO request and the ICMP ECHO reply.[15]
27. **P0F Tool** - This can be used to perform passive fingerprinting.
28. **Port** - A port is an interface where information goes into and out of a computer.
29. **Ports Scanning** - Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what services and applications are open on the target device. Once open, applications or services can be discovered. At this point, further information is typically gathered to determine how best to target any vulnerabilities and weaknesses in the system.[16]
30. **Port number** - TCP/UDP numeric value which serves as identifier to applications and services on systems and each packet/datagram contains source port and destination port.[17]
31. **Port scanner** - Software can be used for searching system for port vulnerabilities. It is also used to determine the state of port to know what applications/services are running.
32. **RST Packet** - is sent either in the middle of the 3-way handshake when the server rejects the connection or is unavailable OR in the middle of data transfer when either the server or client becomes unavailable or rejects further communication without the formal 4-way TCP connection termination process.[18]
33. **Scanning** - This is also known as probing. It is a process of leading the target machines to release useful information about themselves.
34. **Stateful Connection** - is one in which some information about the connection between systems is retained for future use.
35. **Stateless Connection** - There is no session information is retained by the receiver, usually a server.
36. **SYN Packet** - SYN flag synchronizes sequence numbers to initiate a TCP connection.
37. **TCP ACK Scan (-sA)** - This scan is used to determine the firewall rule sets that are being used. When a TCP ACK segment is sent to a closed port, or sent out-of-sync to a listening port, the RFC 793 expected behavior is for the device to respond with an RST. Getting RSTs back in response to an ACK scan gives the attacker useful information that can be used to infer the type of firewall present.[19]

38. **TCP Connect Scan (-sT)** - This is also known as full connect scan. This scan demands the underlying OS to establish a connection with the target machine and port by issuing the connect system call.
39. **TCP SYN Scan (-sS)** - This is also called half-open scan. It is default scan in Nmap and the main concept behind it is TCP three way handshake. Nmap sends a SYN packet and then waits to receive a response. If the ports are open, the scan receives a SYN / ACK flag or a SYN packet in response. If the ports are closed, the system rejects the connection. However, if the ports are filtered, the scan receives no reply.
40. **TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX)** - These three scan types exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports. They are exactly the same in behavior except for the TCP flags set in probe packets.
    - Null scan (-sN): Does not set any bits (TCP flag header is 0)
    - FIN scan (-sF): Sets just the TCP FIN bit.
    - Xmas Tree scan (-sX): Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. Xmas scan is useful for scanning firewalled networks and intrusion detection systems.[20]
41. **TCP 3 Way Handshake** - The client sends a SYN packet which informs the server that the client is likely to start communication and with what sequence number it starts segments with. Then, the server responds to the client's request with SYN-ACK signal bits set. Lastly, the client acknowledges the response of server with an ACK signal and they both establish a reliable connection with which they will start the actual data transfer.[21]
42. **Unfiltered Port** - Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed.[22]
43. **Vulnerability** - This is a weakness or mistake in software or system that can be exploited by an attacker or a hacker to gain access to a system or network.[23]
44. **Vulnerability Assessment** - This is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm.[24]
45. **Vulnerability scanner** - This is a generic term for a range of products that look for vulnerabilities in networks or systems. It is intended to identify vulnerabilities and alert network administrators to these problems. A security administrator would use a vulnerability scanner is to find open ports, software flaws or security misconfigurations on a particular device. Examples of vulnerability scanners are Nessus and Qualys.[25]

46. **Vulnerability scanning** - This is the use of automated software to search a system for known security weaknesses and creates a report of potential exposures. It is a technique that identifies threats on your network, but does not exploit them.[26]
47. **Xmas Tree Port Scan** - Sending a packet with every option set to ON for whatever protocol is in use to observe how a host responds. Xmas scan with reason switch displays the reason a port is in a particular state.[27]
48. **Zenmap** - This is the GUI version of Nmap.

Works Cited

1. "What Is CIDR." *Answers*, Answers Corporation, www.answers.com/Q/What_is_CIDR.
2. NS1 – Intelligent DNS and Traffic Management. "DNS: Types of DNS Records, DNS Servers and DNS Query Types." *NS1*, 24 Apr. 2019, ns1.com/resources/dns-types-records-servers-and-queries.
3. "Damn Vulnerable Web Application." *DVWA*, www.dvwa.co.uk/.
4. "5 Use Tools Such as SuperScan NetBIOS Enumerator and PsTools Suite to Perform." *5 Use Tools Such as SuperScan NetBIOS Enumerator and PsTools Suite to Perform*, www.coursehero.com/file/p75tcnl/5-Use-tools-such-as-SuperScan-NetBIOS-enumerator-and-PsTools-suite-to-perform/.
5. "Chapter 15. Nmap Reference Guide." *Chapter 15. Nmap Reference Guide | Nmap Network Scanning*, nmap.org/book/man.html.
6. "TCP Headers with SYN and FIN Flags Set." *TCP Headers with SYN and FIN Flags Set - TechLibrary - Juniper Networks*, www.juniper.net/documentation/en_US/junos/topics/concept/tcp-syn-fin-flags.html.
7. "Active Network Security Tool." *Hping*, hping.org/.
8. Pratt, Mary K. "What Is an Intrusion Detection System? How an IDS Spots Threats." *CSO Online*, CSO, 19 Feb. 2018, www.csoonline.com/article/3255632/what-is-an-intrusion-detection-system-how-an-ids-spots-threats.html.
9. "Kali Linux." *Amazon*, Amazon, aws.amazon.com/marketplace/pp/Kali-Linux-Kali-Linux/B01M26MMTT.
10. "Netcat." *Wikipedia*, Wikimedia Foundation, 6 June 2019, en.wikipedia.org/wiki/Netcat
11. Angelopoulou, Olga. "ID Theft: A Computer Forensics' Investigation Framework." *Proceedings of The 5 Th Australian Digital Forensics ...*,

www.academia.edu/1048444/ID_Theft_A_Computer_Forensics_Investigation_Framework.
12. Coffey, et al. “Vulnerability Analysis of Network Scanning on SCADA Systems.” *Security and Communication Networks*, Hindawi, 13 Mar. 2018, www.hindawi.com/journals/scn/2018/3794603/.
13. “What Is Packet Filtering? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/4038/packet-filtering.
14. “Packet Loss.” *Wikipedia*, Wikimedia Foundation, 8 June 2019, en.wikipedia.org/wiki/Packet_loss.
15. “What Is Ping Sweep (ICMP Sweep)? - Definition from WhatIs.com.” *SearchNetworking*, searchnetworking.techtarget.com/definition/ping-sweep-ICMP-sweep.
16. “Process: Scanning and Enumeration.” *Infosec Resources*, 25 Nov. 2016, resources.infosecinstitute.com/process-scanning-and-enumeration/.
17. Administrator. “TCP Source & Destination Port Number - Section 1.” *Cisco Networking, VPN Security, Routing, Catalyst-Nexus Switching, Virtualization Hyper-V, Network Monitoring, Windows Server, CallManager, Free Cisco Lab, Linux Tutorials, Protocol Analysis, CCNA, CCNP, CCIE.*, www.firewall.cx/networking-topics/protocols/tcp/133-tcp-source-destination-ports.html.
18. whdwhd 3311 silver badge77 bronze badges, and FarazXFarazX 1. “How Does Load Balancer Manage TCP Connections.” *Server Fault*, serverfault.com/questions/833118/how-does-load-balancer-manage-tcp-connections/833609.
19. “Common Attack Pattern Enumeration and Classification.” *CAPEC*, capec.mitre.org/data/definitions/305.html.
20. *TCP FIN, NULL, and Xmas Scans (-SF, -SN, -SX) | Nmap Network Scanning*, nmap.org/book/scan-methods-null-fin-xmas-scan.html.
21. “Exam 2 Study Guide.” *CS 352 Exam 2 Study Guide*, www.cs.rutgers.edu/~pxk/352/exam/study-guide-2.html.
22. “Chapter 15. Nmap Reference Guide.” *Chapter 15. Nmap Reference Guide | Nmap Network Scanning*, nmap.org/book/man.html.
23. “Vulnerability (Computing).” *Wikipedia*, Wikimedia Foundation, 15 June 2019, en.wikipedia.org/wiki/Vulnerability_(computing).
24. primeteacher32 Follow. “Vulnerability Assessment.” *LinkedIn SlideShare*, 1 Dec. 2015, www.slideshare.net/primeteacher32/vulnerability-assessment-55716203.

25. “Vulnerability Scan.” *Vulnerability Scan - an Overview | ScienceDirect Topics*, www.sciencedirect.com/topics/computer-science/vulnerability-scan.
26. “Cyber Security.” *Wikipedia*, Wikimedia Foundation, 23 Sept. 2017, en.wikipedia.org/wiki/Cyber_security.
27. *Nmap Network Security Scanner Man Page*, svn.nmap.org/!svn/bc/3320/nmap/docs/nmap_manpage.html.