CEH v8 Study Guide

1 **Hardening** is a process the administrators can perform to lock down systems. It includes removing unnecessary software, services, and insecure configuration settings.

2 You might be able to invoke the stored procedure **XP_CMDSHELL** to spawn a windows command shell when attacking MS SQL servers during a penetration test.

3 When analyzing IDS logs, one challenge is dealing with **false positives**. An example of this is an administrator who accesses an external router from his/her computer, then immediately noticed this authorized action caused an alert in the IDS.

4 If you discover a new critical flaw in software, such as a bug in word processing software which causes the system to crash upon entering a certain key sequence, you should **notify the vendor of the bug and do not disclose it until the vendor gets a chance to fix the issue.**

5 Most operating systems perform a one-way hash against passwords to protect the passwords while they are being stored. Essentially the actual password is never stored, but only the one way hash which uniquely represents the password is stored.

6 If you get a response back from **Firewalk** that says the following; TCP port 78 – no response, TCP port 79 – no response, **TCP port 80 – Time-to-live exceeded. This tells us that port 80 is open on the firewall.**

7 **Facial recognition scan** technology measures a person's external features through a digital video camera.

8 **Collision Resistance** is a property that ensures that a hash function will not produce the same hashed value for two different messages or data.

9 A **Boot Sector Virus** overwrites the original MBR (master boot record), and only executes the new virus code and not the original boot record.

10 **UDP Port 514** may be used to log messages to a log analysis tool that resides behind a firewall. This port is often used for Syslog.

11 When dealing with risks, a decision maker may choose to **mitigate the risk**. Rejecting or denying the risk are not acceptable options.

12 Nmap can be used to do some basic vulnerability scanning functions by invoking the **Nmap Scripting Engine** (NSE) resource.

13 **Active OS fingerprinting** sends specially crafted packets to the remote OS and analyzes the received responses.

14 **A Bollard** is a strong post designed to stop a car from breaching a predefined boundary.

15 Concerning **proxy firewalls**, computers establish a connection with a proxy firewall, which then initiates a new network connection for the client.

16 Using a **USB Token and PIN** combination for authentication is an example of **two-factor authentication**. The USB token is something you have, while the PIN is something you know.

17 The difference between symmetric and asymmetric cryptography is **symmetric** cryptography uses **the same key on each end of the transmission medium**, whereas asymmetric does not.

18 Storing passwords in the form of **hashes** is appropriate because hashes are considered to **one-way or non-reversible** which makes finding the password being represented much more difficult.

19 To **find which ip addresses are active on the network**, a hacker could use the nmap switch of –**sP** which initiates a **ping scan**.

20 The code **IMG SRC=vbscript : msgbox("Vulnerable") ; > originalAttribute="SRC" originalPath= "vbscript: msgbox("Vulerable");>"** is an example of a **Cross-Site Request Forgery** attack.

21 The **Connection Stream Parameter Pollution Attack** is a method where the attacker is **injecting parameters into a connection string using semicolons as a**

separator. It's mostly targeted at poor security between web applications and backend databases.

22 A security **procedure document** is written with **specific step-by-step details**. This makes it different from a security policy document or security recommendations document.

23 **Bluetooth** uses **FSK or Frequency-Shift Keying** as its digital modulation technique to exchange information between paired devices.

24 **Using a Covert Channel** is when an attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information.

25 **ICMP Ping and Ping Sweeps** are used to check for active systems and to check the number of hops an ICMP ping takes to teach a destination.

26 If you wanted to (or a hacker wanted to) use **nslookup** to query DNS (Domain Name Service) for dns information or servers, he/she would first have to set a type using the set type command. For example to query for dns servers, the set up **nslookup** for querying name servers, the command would be **set type=ns.**

27 **Non-repudiation** is a principle that prevents a party from denying its role in a given activity.

28 An nmap scan result showing **port 69** being open could pose the risk of **unauthenticated access**. Port 69 being open usually means tftp is in use. This is more specifically related to UDP 69.

29 The only way to truly verify that a tape backup can be entirely recovered is to do a **Full Restore**.

30 **The Service Oriented Architecture (SOA)** has better performance concerning secure communications when using **WS-SecureConversation** as its setting.

31 When setting up wireless security and using a pre-shared key solution such as WEP or WPA, the security key entered is symmetric and is what is used to encrypt the wireless data. NOTE: Same key is also used for decrypting.

32 **Zero-day or 0day vulnerabilities** are ones that have not been disclosed to the general public or software vendor.

33 **Cross Certification** must be established for one CA to trust another, such as when two companies with individual PKI's merge with each other.

34 The sender must have the recipient's **Public Key** to send the recipient a PGP encrypted message.

35 If a company is using **Windows 2003 Active Directory** for directory services, a **Rainbow Table** based attack is the most efficient way to crack the company's Active Directory passwords.

36 When using **LANMAN** hashing, if the password hashed is **7 characters or less,** the second half of the hash will always be **0xAAD3B435B51404EE**.

37 **Combining solutions** such as email gateways, desktop anti-virus and other solutions is an effective way to **mitigate social engineering attacks.**

38 If an organization, such as a bank, handles privacy information and has never used the auditing features of its systems, the first step they should perform is to determine the impact of enabling the audit features.

39 The Open Web Application Security Project released an application full of known security vulnerabilities named **WebGoat** for the sake of testing and education.

40 If you are using **AES** as your encryption of choice for sending a secure message, you must use a **shared key** for encryption, since AES is a symmetric algorithm.

41 **SHA-1,** which uses **160 bit** message digest, is better for protecting against brute forcing than MD5.

42 Shrinking event log size is one sign of a potential attack. When incidents like that occur an administrator would consult their site security policy and follow its recommendations.

43 **Covert Channels** are commonly used to defeat multi-level security systems to do such operations as leak sensitive data.

44 **Tripwire** is a **file integrity verifier** that can be used to detect unauthorized changes to binary files on a system.

45 The **WPA2 authentication handshake** is vulnerable to **attack/cracking**.

46 To successfully exploit a Cross Site Scripting vulnerability, cookies must NOT have the httponly flag set.

47 Breaking into the email of a husband or wife is never considered to be an “Ethical” action, when it’s being requested by either the husband or wife.

48 To do an Nmap **syn stealth** scan you would use the **–sS** switch. For example, nmap –sS –O 192.168.1.1 –p 80,443 would do a syn stealth scan to ports 80 and 443, while also attempting to do an **OS identification** operation per the **–O** option.

49 **Usbdumper** can be used to silently/stealthily copy data from a usb drive.

50 When checking for SQL injection, it is a common first step to try and use a single quote to break a valid SQL Request.

51 Strong **mutual authentication** can be used to minimize the threat of **man-in-the-middle attacks.**

52 **Nmap** is one of the best choices for scanning the network to find potential target systems.

53 **A Gateway** is best described as a device that relays packets between disparate networks, such as a WAN and LAN.

54 There is no tip 54.

55 4[20/Mar/2011:10:49;07] “GET /login.php?user=test’+oR+3>2%20- - HTTP/1.1” is an example of a SQL Injection attack. The code below is vulnerable to SQL Injection.

```
php
include(‘../../config/db_connect.php’);
$user = $_GET[‘user’];
$pass = $_GET[‘pass’];
$sql = “SELECT * FROM USERS WHERE username = ‘$user’ AND password =          ‘$pass’”;
$result = mysql_query($sql) or die (“couldn’t execute query”);

if (mysql_num_rows($result) != 0 ) echo  ‘Authentication granted!’;
else echo ‘Authentication failed!’;
?>
```

56 A **Top Down** approach is used for security program management if senior management is supporting and enforcing the security policy.

57 A hacker may search google for **pcf files to find Cisco VPN config files**. Those files may contain connectivity passwords that can be decoded with **Cain and Abel**

58 An ethical hacker should sign a Non Disclosure agreement before performing any other actions when being brought into an organization to access security.

59 If you're using **Metasploit** and you exploit an FTP server for example and want to **pivot** to an internal or dmz lan, you'd use meterpreter to create a **route statement**.

60 **Advanced encryption standard (AES)** is an algorithm used primarily for **Bulk Data Encryption.**

61 **John the Ripper** is one of the fastest and most efficient **password crackers.**

62 A newly discovered flaw in a software application is also called **0-day.**

63 When hosting internal intranets and web applications that may be reachable from the internet, one technique to minimize enumeration vulnerabilities is to remove A records that point to internal hosts from DNS servers reachable from outside.

64 The broadcast address for the subnet 190.86.168.0/22 would be 192.86.168.255.

65 An **Audit Trail** is an example of a **detective control**.

66 Running the netcat command **nc-| -p 2222 | nc 10.1.0.43 1234** will cause netcat to listen on port 2222 and output anything received to a remote connection on 10.1.0.43 over port 1234

67 If you are able to reach websites by ip address but not by domain name, either the dns server is down, or **you need to open tcp and udp port 53 on the firewall**.

68 Printing out pentest reports or audits of previous companies is not recommended as a method of showing proof of work to new companies.

69 When investigating IDS alerts, a security professional should investigate based on the potential effect of the incident.

70 A technique that pulls passwords from a list of commonly used passwords to try against a secured PDF until the correct password is found or the list is exhausted is an example of a Dictionary Attack (password crack).

71 **Sniffing** can be broadly categorized as **Active and/or Passive**.

72 **Mac Flood** attack is one way to **sniff in a switched environment**.

73 Scripting languages are typically slower than compiled languages as scripting languages require an interpreter to run its code.

74 A **Honeypot** can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions. It's often used to fool hackers or study their activities.

75 **Rule based access control** is used on a router or firewall to limit network activity

76 **WPA2** uses **AES** for wireless data encryption at **128 bit and CCMP** level.

77 **Social Engineering testing** would be most effective in determining whether end-user security training would be beneficial

78 **Arp Spoofing, Mac Flooding, and Mac Duplication** are techniques that can be used to enable an attacker to sniff on a switched network.

79 **BGP (Border Gateway Protocol)** is a common protocol used by routers.

80 **The Principle of Least Privilege** primarily ensures that users or other entities only have the permissions/privileges required for legitimate job related purposes.

81 If you work as a pentester for a company, before engaging in penetration tests outside of the ones performed for the company you work for, you should seek written permission from that company.

82 **Stored Biometric** technologies are vulnerable to attack primarily due to the fact that if an attacker gains access to the stored biometric information, it can be used to impersonate a legitimate user.

83 Patterns in time gaps in system and/or event logs, New user accounts created, and an increased amount of failed logon events are all common signs that a system has been compromised or hacked.

84 To perform **OS Detection** with nmap the **–O** switch should be used. (capital O)

85 A **botnet** can be managed and controlled through **IRC channels**.

86 **Missing Patches** is a common vulnerability that exposes sensitive data stored on Windows Servers.

87 The main advantage to using older **packet filtering routers** is that they are fast, flexible and have minimum impact on network performance.

88 **PCI – DSS** compliance requires a penetration test at least once a year and after any significant system modification, upgrade, or replacement.

89 **A Network Tap** combined with Wireshark would allow one to capture ALL traffic on the wire.

90 **IKE-Scan** is useful for fingerprinting VPN firewalls.

91 On a network mixed with Windows and Linux, sending a ping to the **broadcast address**, for example 192.168.1.**255,** would result in only the Linux machines responding as Windows does not respond to broadcast pings.

92 Information gathered from social networking websites such as **Facebook, Twitter and LinkedIn** can be used to launch **Social Engineering attacks, and Phishing attacks.**

93 **Snort** can be configured to run in three modes; **Sniffing, Logging, and Network Intrusion Detection System.**

94 **Nessus** can help with compliance concerning PCI Requirement 11.

95 When an IDS **should be generating alerts but does not**, this is known as a **False Negative.**

96 **Change Management** ensures that updates to policies, procedures and configurations are made in a controlled and documented fashion.

97 **The Global Variable Settings** configuration in Nessus is found on the Plugins tab.

98 **3DES (Triple DES)** is a symmetric cryptographic standard.

99 **Run services in least privilege mode** to defend against privilege escalation. Also using multi-factor authentication and authorization can help.

100 **PGP** is an example of an asymmetric encryption implementation.

101 **Disabling a router from accepting broadcast pings** is one way to protect the router or network from Smurf attacks.

102 In a PKI the **Registration Authority** verifies the applicant.

103 **The Trusted Network Interpretation Environments Guideline** provides direction on security protection measures required in different network environments.

104 In PKI the CA is the trusted Root that issues certificates.

105 **TCP-OVER-DNS** is a client-server tool used to evade firewall inspection.

106 **Timing Options** can be adjusted when running Nmap to slow down a scan to perhaps aid in evading IDS and other monitoring.

107 If you run an **Nmap Ack scan** against a gateway device against a specific port and the results come back to say the port is **unfiltered**, it usually means **Stateless Filtering** is happening.

108 Vulnerability scanners usually detect vulnerabilities in services by **analyzing service responses**.

109 **Hidden Form Fields** are often attacked to make purchases on websites without paying the proper price for the purchase.

110 **Replay Attacks** are often used when public key cryptography has been used.

111 An administrator's **RDP Login** traffic could be captured and decoded with **Cain and Abel.**

112 The command **telnet webserverAddress 80 HEAD / HTTP/1.0** could be used to fingerprint a web server.

113 The following Nmap command is an example of a Stealth Scan; **nmap –n –sS –P0 –p 80.** The –n tells Nmap not to perform name resolution, the –sS tells nmap to do a Syn Stealth Scan, the –P0 (zero) tells Nmap not to ping the target (which it does by default) and the –p 80 tells Nmap to scan port 80.

114 A **security policy** will be more accepted by employees if it is consistent and has the support of **executive management**.

115 The three types/factors of **authentication** are **something you: have, know, are.**

116 Passive reconnaissance involves collecting information through publicly accessible sources.