

Exam Questions 312-50v11

Certified Ethical Hacker Exam (CEH v11)

<https://www.2passeasy.com/dumps/312-50v11/>



NEW QUESTION 1

Why containers are less secure than virtual machines?

- A. Host OS on containers has a larger surface attack.
- B. Containers may full fill disk space of the host.
- C. A compromise container may cause a CPU starvation of the host.
- D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 2

Study the following log extract and identify the attack.

- A. Hexcode Attack
- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

Answer: D

NEW QUESTION 3

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

- A. wireshark --fetch "192.168.8*"
- B. wireshark --capture --local masked 192.168.8.0 ---range 24
- C. tshark -net 192.255.255.255 mask 192.168.8.0
- D. sudo tshark -f"net 192.168.8.0/24"

Answer: D

NEW QUESTION 4

Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32-bit encryption.
- D. Effective length is 7 characters.

Answer: ABD

NEW QUESTION 5

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- A. SOA
- B. biometrics
- C. single sign on
- D. PKI

Answer: D

NEW QUESTION 6

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

- A. http-methods
- B. http enum
- C. http-headers
- D. http-git

Answer: A

NEW QUESTION 7

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 8

Which of the following Linux commands will resolve a domain name into IP address?

- A. >host-t a hackeddomain.com
- B. >host-t ns hackeddomain.com
- C. >host -t soa hackeddomain.com
- D. >host -t AXFR hackeddomain.com

Answer: A

NEW QUESTION 9

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

- A. Create an incident checklist.
- B. Select someone else to check the procedures.
- C. Increase his technical skills.
- D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 10

Which of the following tools can be used to perform a zone transfer?

- A. NSLookup
- B. Finger
- C. Dig
- D. Sam Spade
- E. Host
- F. Netcat
- G. Neotrace

Answer: ACDE

NEW QUESTION 10

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

- A. Iris patterns
- B. Voice
- C. Height and Weight
- D. Fingerprints

Answer: C

NEW QUESTION 11

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Answer: D

NEW QUESTION 14

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Answer: A

NEW QUESTION 18

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised. What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack

Answer: A

NEW QUESTION 20

Scenario1:

- * 1. Victim opens the attacker's web site.
 - * 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'.
 - * 3. Victim clicks to the interesting and attractive content URL.
 - * 4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make \$1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
- What is the name of the attack which is mentioned in the scenario?

- A. Session Fixation
- B. HTML Injection
- C. HTTP Parameter Pollution
- D. Clickjacking Attack

Answer: D

NEW QUESTION 21

Which of the following is the BEST way to defend against network sniffing?

- A. Using encryption protocols to secure network communications
- B. Register all machines MAC Address in a Centralized Database
- C. Use Static IP Address
- D. Restrict Physical Access to Server Rooms hosting Critical Servers

Answer: A

NEW QUESTION 23

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

- A. nslookup -fullrecursive update.antivirus.com
- B. dnsnooping -rt update.antivirus.com
- C. nslookup -norecursive update.antivirus.com
- D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 28

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

Answer: C

NEW QUESTION 29

```
env x='(){ :};echo exploit' bash -c 'cat/etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Removes the passwd file
- B. Changes all passwords in passwd
- C. Add new user to the passwd file
- D. Display passwd content to prompt

Answer: D

NEW QUESTION 30

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

Answer: A

NEW QUESTION 32

What port number is used by LDAP protocol?

- A. 110
- B. 389
- C. 464
- D. 445

Answer: B

NEW QUESTION 35

Nedved is an IT Security Manager of a bank in his country. One day, he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?

- A. Leave it as it is and contact the incident response team right away
- B. Block the connection to the suspicious IP Address from the firewall
- C. Disconnect the email server from the network
- D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 38

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He's determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

- A. Error-based SQL injection
- B. Blind SQL injection
- C. Union-based SQL injection
- D. NoSQL injection

Answer: B

NEW QUESTION 43

What is the proper response for a NULL scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

Answer: F

NEW QUESTION 47

In Trojan terminology, what is a covert channel?

- A. A channel that transfers information within a computer system or network in a way that violates the security policy
- B. A legitimate communication path within a computer system or network for transfer of data
- C. It is a kernel operation that hides boot processes and services to mask detection
- D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Answer: A

NEW QUESTION 48

Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

- A. All of the employees would stop normal work activities
- B. IT department would be telling employees who the boss is
- C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
- D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 53

What did the following commands determine?

- A. That the Joe account has a SID of 500
- B. These commands demonstrate that the guest account has NOT been disabled
- C. These commands demonstrate that the guest account has been disabled
- D. That the true administrator is Joe
- E. Issued alone, these commands prove nothing

Answer: D

NEW QUESTION 56

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

Answer: B

NEW QUESTION 57

What tool can crack Windows SMB passwords simply by listening to network traffic?

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

Answer: D

NEW QUESTION 59

One of your team members has asked you to analyze the following SOA record.

What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400

E. 60
F. 4800

Answer: D

NEW QUESTION 62

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 67

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

- A. 110
- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

Answer: BCE

NEW QUESTION 72

You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

- A. user.log
- B. auth.fesg
- C. wtmp
- D. btmp

Answer: C

NEW QUESTION 76

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

- A. False negative
- B. True negative
- C. True positive
- D. False positive

Answer: D

NEW QUESTION 78

Trempe is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Trempe's requirements?

- A. Gateway-based IDS
- B. Network-based IDS
- C. Host-based IDS
- D. Open source-based

Answer: C

NEW QUESTION 81

What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premier environment

- A. VCloud based
- B. Honypot based
- C. Behaviour based
- D. Heuristics based

Answer: A

NEW QUESTION 83

Which of the following statements about a zone transfer is correct? (Choose three.)

- A. A zone transfer is accomplished with the DNS
- B. A zone transfer is accomplished with the nslookup service
- C. A zone transfer passes all zone information that a DNS server maintains
- D. A zone transfer passes all zone information that a nslookup server maintains
- E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
- F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 85

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTICTLS
- B. UPGRADETLS
- C. FORCETLS
- D. STARTTLS

Answer: D

NEW QUESTION 86

What is the proper response for a NULL scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

Answer: E

NEW QUESTION 87

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 113
- B. 69
- C. 123
- D. 161

Answer: C

NEW QUESTION 92

An attacker runs netcat tool to transfer a secret file between two hosts.

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
- B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
- C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
- D. Use cryptcat instead of netcat

Answer: D

NEW QUESTION 93

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Use a scan tool like Nessus
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Answer: B

NEW QUESTION 95

Study the snort rule given below:

From the options below, choose the exploit against which this rule applies.

- A. WebDav
- B. SQL Slammer
- C. MS Blaster

D. MyDoom

Answer: C

NEW QUESTION 100

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

- A. Clickjacking
- B. Cross-Site Scripting
- C. Cross-Site Request Forgery
- D. Web form input validation

Answer: C

NEW QUESTION 103

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

- A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
- B. Connect to the site using SSL, if you are successful then the website is genuine
- C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
- D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
- E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

Answer: C

NEW QUESTION 105

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. DynDNS
- B. DNS Scheme
- C. DNSSEC
- D. Split DNS

Answer: D

NEW QUESTION 109

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
- B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- C. Symmetric encryption allows the server to security transmit the session keys out-of-band.
- D. Asymmetric cryptography is computationally expensive in compariso
- E. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Answer: A

NEW QUESTION 112

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Application
- B. Transport
- C. Session
- D. Presentation

Answer: D

NEW QUESTION 113

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

Answer: B

NEW QUESTION 114

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

- A. The host is likely a Linux machine.
- B. The host is likely a printer.
- C. The host is likely a router.
- D. The host is likely a Windows machine.

Answer: B

NEW QUESTION 115

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

- A. The switches will drop into hub mode if the ARP cache is successfully flooded.
- B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
- C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
- D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 120

Which type of sniffing technique is generally referred as MiTM attack?

- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

Answer: B

NEW QUESTION 123

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

NEW QUESTION 124

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 127

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking. What should you do?

- A. Confront the client in a respectful manner and ask her about the data.
- B. Copy the data to removable media and keep it in case you need it.
- C. Ignore the data and continue the assessment until completed as agreed.
- D. Immediately stop work and contact the proper legal authorities.

Answer: D

NEW QUESTION 132

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

- A. Take over the session
- B. Reverse sequence prediction
- C. Guess the sequence numbers
- D. Take one of the parties offline

Answer: C

NEW QUESTION 136

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- A. openssl s_client -site www.website.com:443
- B. openssl_client -site www.website.com:443
- C. openssl s_client -connect www.website.com:443
- D. openssl_client -connect www.website.com:443

Answer: C

NEW QUESTION 138

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 142

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

- A. tcpsplice
- B. Burp
- C. Hydra
- D. Whisker

Answer: D

NEW QUESTION 144

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Answer: ABD

NEW QUESTION 149

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively
- C. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- D. Test automation is not usable in security due to the complexity of the tests.
- E. It can accelerate benchmark tests and repeat them with a consistent test setu
- F. But it cannot replace manual testing completely.

Answer: D

NEW QUESTION 153

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Digest
- B. Secret Key
- C. Public Key
- D. Hash Algorithm

Answer: C

NEW QUESTION 155

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Service Level Agreement
- B. Project Scope
- C. Rules of Engagement
- D. Non-Disclosure Agreement

Answer: C

NEW QUESTION 159

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

Answer: C

NEW QUESTION 160

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

Answer: D

NEW QUESTION 165

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

Answer: C

NEW QUESTION 166

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Answer: B

NEW QUESTION 169

What is the purpose of DNS AAAA record?

- A. Authorization, Authentication and Auditing record
- B. Address prefix record
- C. Address database record
- D. IPv6 address resolution record

Answer: D

NEW QUESTION 173

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist
- C. Mantrap
- D. Turnstile

Answer: A

NEW QUESTION 177

Which service in a PKI will vouch for the identity of an individual or company?

- A. KDC
- B. CR
- C. CBC
- D. CA

Answer: D

NEW QUESTION 178

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

From the above list identify the user account with System Administrator privileges.

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Answer: F

NEW QUESTION 182

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 184

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

Answer: A

NEW QUESTION 188

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

- A. The use of security agents in clients' computers
- B. The use of DNSSEC
- C. The use of double-factor authentication
- D. Client awareness

Answer: B

NEW QUESTION 193

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS
- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

Answer: D

NEW QUESTION 198

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to access the user and password information stored in the company's SQL database.
- B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
- C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
- D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Answer: B

NEW QUESTION 199

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

- A. Multi-cast mode
- B. Promiscuous mode
- C. WEM
- D. Port forwarding

Answer: B

NEW QUESTION 202

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

- A. tcp.port == 21
- B. tcp.port == 23
- C. tcp.port == 21 || tcp.port == 22
- D. tcp.port != 21

Answer: A

NEW QUESTION 203

Which of the following are well known password-cracking programs?

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Answer: AE

NEW QUESTION 205

The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

- A. The CFO can use a hash algorithm in the document once he approved the financial statements
- B. The CFO can use an excel file with a password
- C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document

- A. C#
- B. Python
- C. Java
- D. C++

Answer: D

NEW QUESTION 228

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Answer: C

NEW QUESTION 231

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

- A. Black-Hat Hackers A
- B. Script Kiddies
- C. White-Hat Hackers
- D. Gray-Hat Hacker

Answer: C

NEW QUESTION 232

Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

- A. Protect the payload and the headers
- B. Encrypt
- C. Work at the Data Link Layer
- D. Authenticate

Answer: D

NEW QUESTION 237

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.

You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

- A. The buffer overflow attack has been neutralized by the IDS
- B. The attacker is creating a directory on the compromised machine
- C. The attacker is attempting a buffer overflow attack and has succeeded
- D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

NEW QUESTION 238

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach.

After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

- A. Although the approach has two phases, it actually implements just one authentication factor
- B. The solution implements the two authentication factors: physical object and physical characteristic
- C. The solution will have a high level of false positives
- D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 242

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Answer: A

NEW QUESTION 243

What is the minimum number of network connections in a multihomed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Answer: A

NEW QUESTION 246

Which of the following is the best countermeasure to encrypting ransomwares?

- A. Use multiple antivirus softwares
- B. Pay a ransom
- C. Keep some generation of off-line backup
- D. Analyze the ransomware to get decryption key of encrypted data

Answer: C

NEW QUESTION 248

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Transport layer port numbers and application layer headers
- B. Presentation layer headers and the session layer port numbers
- C. Network layer headers and the session layer port numbers
- D. Application layer port numbers and the transport layer headers

Answer: A

NEW QUESTION 253

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation
- C. Dynamic Network Address Translation
- D. Static Network Address Translation

Answer: D

NEW QUESTION 256

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

- A. \$1320
- B. \$440
- C. \$100
- D. \$146

Answer: D

NEW QUESTION 261

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

NEW QUESTION 263

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed

by other users.

- A. LDAP Injection attack
- B. Cross-Site Scripting (XSS)
- C. SQL injection attack
- D. Cross-Site Request Forgery (CSRF)

Answer: B

NEW QUESTION 265

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what driver and library are required to allow the NIC to work in promiscuous mode?

- A. Libpcap
- B. Awinpcap
- C. Winprom
- D. Winpcap

Answer: D

NEW QUESTION 269

During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

- A. Private keys
- B. User passwords
- C. Public keys
- D. Public and private keys

Answer: C

NEW QUESTION 273

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy
- B. BBProxy
- C. Blooover
- D. BBCrack

Answer: B

NEW QUESTION 274

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 276

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

Answer: D

NEW QUESTION 277

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. nessus
- B. tcpdump
- C. ethereal
- D. jack the ripper

Answer: B

NEW QUESTION 280

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their

job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- A. MAC Flooding
- B. Smurf Attack
- C. DNS spoofing
- D. ARP Poisoning

Answer: C

NEW QUESTION 285

What is the main security service a cryptographic hash provides?

- A. Integrity and ease of computation
- B. Message authentication and collision resistance
- C. Integrity and collision resistance
- D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 287

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.

However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

Answer: B

NEW QUESTION 289

Which regulation defines security and privacy controls for Federal information systems and organizations?

- A. HIPAA
- B. EU Safe Harbor
- C. PCI-DSS
- D. NIST-800-53

Answer: D

NEW QUESTION 292

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

- A. ACK
- B. SYN
- C. RST
- D. SYN-ACK

Answer: B

NEW QUESTION 293

The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?

- A. network Sniffer
- B. Vulnerability Scanner
- C. Intrusion prevention Server
- D. Security incident and event Monitoring

Answer: D

NEW QUESTION 298

What is the following command used for? `net use \targetip$ "" /u:""`

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

Answer: D

NEW QUESTION 300

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- A. Passwords
- B. File permissions
- C. Firewall rulesets
- D. Usernames

Answer: A

NEW QUESTION 301

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

Answer: B

NEW QUESTION 306

Which definition among those given below best describes a covert channel?

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.
- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure

Answer: B

NEW QUESTION 309

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

Answer: A

NEW QUESTION 310

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

Answer: B

NEW QUESTION 312

Why is a penetration test considered to be more thorough than vulnerability scan?

- A. Vulnerability scans only do host discovery and port scanning by default.
- B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
- C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
- D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Answer: B

NEW QUESTION 313

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v11 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v11 Product From:

<https://www.2passeasy.com/dumps/312-50v11/>

Money Back Guarantee

312-50v11 Practice Exam Features:

- * 312-50v11 Questions and Answers Updated Frequently
- * 312-50v11 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v11 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v11 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year