# Exam Questions CEH-001

Certified Ethical Hacker (CEH)

**https://www.2passeasy.com/dumps/CEH-001/**

**NEW QUESTION 1**
- (Topic 1)
Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

A. Neil will have to configure a Bridged port that will copy all packets to the protocol analyzer.
B. Neil will need to setup SPAN port that will copy all network traffic to the protocol analyzer.
C. He will have to setup an Ether channel port to get a copy of all network traffic to the analyzer.
D. He should setup a MODS port which will copy all network traffic.

**Answer:** B

**NEW QUESTION 2**
- (Topic 1)
David is a security administrator working in Boston. David has been asked by the office's manager to block all POP3 traffic at the firewall because he believes employees are spending too much time reading personal email. How can David block POP3 at the firewall?

A. David can block port 125 at the firewall.
B. David can block all EHLO requests that originate from inside the office.
C. David can stop POP3 traffic by blocking all HELO requests that originate from inside the office.
D. David can block port 110 to block all POP3 traffic.

**Answer:** D

**NEW QUESTION 3**
- (Topic 1)
Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Configure Port Security on the switch
B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch

**Answer:** A

**NEW QUESTION 4**
- (Topic 1)
A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.

What privilege level does a rootkit require to infect successfully on a Victim's machine?

A. User level privileges
B. Ring 3 Privileges
C. System level privileges
D. Kernel level privileges

**Answer:** D

**NEW QUESTION 5**
- (Topic 1)
You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.
Here is the output of your scan results:

Which of the following nmap command did you run?

A. nmap -A -sV -p21, 110, 123 10.0.0.5
B. nmap -F -sV -p21, 110, 123 10.0.0.5
C. nmap -O -sV -p21, 110, 123 10.0.0.5
D. nmap -T -sV -p21, 110, 123 10.0.0.5

**Answer:** C

**NEW QUESTION 6**
- (Topic 1)
Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.
No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.
What type of insider threat would Shayla be considered?

A. She would be considered an Insider Affiliate
B. Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate

C. Shayla is an Insider Associate since she has befriended an actual employee
D. Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider

**Answer:** A

**NEW QUESTION 7**
- (Topic 1)
Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

A. Ursula would be considered a gray hat since she is performing an act against illegal activities.
B. She would be considered a suicide hacker.
C. She would be called a cracker.
D. Ursula would be considered a black hat.

**Answer:** B

**NEW QUESTION 8**
- (Topic 1)
Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". 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 9**
- (Topic 1)
Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible?

A. It works because encryption is performed at the application layer (single encryption key)
B. The scenario is invalid as a secure cookie cannot be replayed
C. It works because encryption is performed at the network layer (layer 1 encryption)
D. Any cookie can be replayed irrespective of the session status

**Answer:** A

**NEW QUESTION 10**
- (Topic 1)
The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
How will you delete the OrdersTable from the database using SQL Injection?

A. Chicago'; drop table OrdersTable --
B. Delete table'blah'; OrdersTable --
C. ; SELECT * OrdersTable > DROP --
D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

**Answer:** A

**NEW QUESTION 10**
- (Topic 1)
Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results. The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.
Which of the below Google search string brings up sites with "config.php" files?

A. Search:index config/php
B. Wordpress:index config.php
C. intitle:index.of config.php
D. Config.php:index list

**Answer:** C

**NEW QUESTION 12**
- (Topic 1)
You receive an e-mail with the following text message.
"Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".
What category of virus is this?

A. Virus hoax
B. Spooky Virus
C. Stealth Virus
D. Polymorphic Virus

**Answer:** A

**NEW QUESTION 13**
- (Topic 1)
What port number is used by Kerberos protocol?

A. 88
B. 44
C. 487
D. 419

**Answer:** A

**NEW QUESTION 15**
- (Topic 1)

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.
Where can Stephanie go to see past versions and pages of a website?

A. She should go to the web page Samspade.org to see web pages that might no longer be on the website
B. If Stephanie navigates to Search.com; she will see old versions of the company website
C. Stephanie can go to Archive.org to see past versions of the company website
D. AddressPast.com would have any web pages that are no longer hosted on the company's website

**Answer:** C

**NEW QUESTION 16**
- (Topic 1)
Which type of hacker represents the highest risk to your network?

A. black hat hackers
B. grey hat hackers
C. disgruntled employees
D. script kiddies

**Answer:** C

**NEW QUESTION 21**
- (Topic 1)
This tool is widely used for ARP Poisoning attack. Name the tool.

A. Cain and Able
B. Beat Infector
C. Poison Ivy
D. Webarp Infector

**Answer:** A

**NEW QUESTION 24**
- (Topic 1)
One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

A. Set up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process
B. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack
C. Replicating servers that can provide additional failsafe protection
D. Load balance each server in a multiple-server architecture

**Answer:** A

**NEW QUESTION 27**
- (Topic 1)
Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on
its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes
? Everything you search for using Google
? Every web page you visit that has Google Adsense ads
How would you prevent Google from storing your search keywords?

A. Block Google Cookie by applying Privacy and Security settings in your web browser
B. Disable the Google cookie using Google Advanced Search settings on Google Search page
C. Do not use Google but use another search engine Bing which will not collect and store your search keywords
D. Use MAC OS X instead of Windows 7. Mac OS has higher level of privacy controls by default.

**Answer:** A

**NEW QUESTION 31**
- (Topic 1)

In which part of OSI layer, ARP Poisoning occurs?

A. Transport Layer
B. Datalink Layer
C. Physical Layer
D. Application layer

**Answer:** B

**NEW QUESTION 33**
- (Topic 1)
This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning

**Answer:** B

**NEW QUESTION 36**
- (Topic 1)
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

A. The source and destination address having the same value
B. A large number of SYN packets appearing on a network without the corresponding reply packets
C. The source and destination port numbers having the same value
D. A large number of SYN packets appearing on a network with the corresponding reply packets

**Answer:** B

**NEW QUESTION 41**
- (Topic 1)
BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.
BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.

What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim's machine?

A. Physical access - the attacker can simply copy a Trojan horse to a victim's hard disk infecting the machine via Firefox add-on extensions
B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
E. Downloading software from a website? An attacker can offer free software, such as shareware programs and pirated mp3 files

**Answer:** E

**NEW QUESTION 42**
- (Topic 1)
You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS streams. How will you accomplish this?

A. copy secret.txt c:\windows\system32\tcpip.dll kernel>secret.txt
B. copy secret.txt c:\windows\system32\tcpip.dll:secret.txt
C. copy secret.txt c:\windows\system32\tcpip.dll |secret.txt
D. copy secret.txt >< c:\windows\system32\tcpip.dll kernel secret.txt

**Answer:** B

**NEW QUESTION 43**
- (Topic 1)
In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

A. Full Blown Attack
B. Thorough Attack
C. Hybrid Attack
D. BruteDict Attack

**Answer:** C

**NEW QUESTION 45**
- (Topic 1)
In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:
FIN = 1
SYN = 2
RST = 4
PSH = 8
ACK = 16
URG = 32
ECE = 64
CWR = 128
Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.

What is Jason trying to accomplish here?

A. SYN, FIN, URG and PSH
B. SYN, SYN/ACK, ACK
C. RST, PSH/URG, FIN
D. ACK, ACK, SYN, URG

**Answer:** B

**NEW QUESTION 47**
- (Topic 1)
You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

A. New installation of Windows should be patched by installing the latest service packs and hotfixes
B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed
C. Install a personal firewall and lock down unused ports from connecting to your computer
D. Install the latest signatures for Antivirus software
E. Configure "Windows Update" to automatic
F. Create a non-admin user with a complex password and logon to this account
G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

**Answer:** ACDEF

**NEW QUESTION 52**
- (Topic 1)
Which Steganography technique uses Whitespace to hide secret messages?

A. snow

B. beetle
C. magnet
D. cat

**Answer:** A

**NEW QUESTION 53**
- (Topic 1)
This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

A. Wiresharp attack
B. Switch and bait attack
C. Phishing attack
D. Man-in-the-Middle attack

**Answer:** C

**NEW QUESTION 55**
- (Topic 1)
Consider the following code:
URL:http://www.certified.com/search.pl? text=<script>alert(document.cookie)</script>
If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.
What is the countermeasure against XSS scripting?

A. Create an IP access list and restrict connections based on port number
B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts
C. Disable Javascript in IE and Firefox browsers
D. Connect to the server using HTTPS protocol instead of HTTP

**Answer:** B

**NEW QUESTION 56**
- (Topic 1)
Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system.
Which of the following is NOT an example of default installation?

A. Many systems come with default user accounts with well-known passwords that administrators forget to change
B. Often, the default location of installation files can be exploited which allows a hacker to retrieve a file from the system
C. Many software packages come with "samples" that can be exploited, such as the sample programs on IIS web services
D. Enabling firewall and anti-virus software on the local system

**Answer:** D

**NEW QUESTION 60**
- (Topic 1)
In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design
B. Elimination
C. Incorporation
D. Replication
E. Launch
F. Detection

**Answer:** E

**NEW QUESTION 64**
- (Topic 1)
This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor- intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly

**Answer:** C

**NEW QUESTION 65**
- (Topic 1)
Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to

send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities.
What are some of the common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities
B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

**Answer:** A

**NEW QUESTION 70**
- (Topic 1)
Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping

**Answer:** A

**NEW QUESTION 75**
- (Topic 1)
What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilities than more esoteric ones
B. The scanning speed of their scanners are extremely high
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
D. The more vulnerabilities detected, the more tests required
E. They are highly expensive and require per host scan license

**Answer:** AC

**NEW QUESTION 79**
- (Topic 1)
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
B. Educate and enforce physical security policies of the company to all the employees on a regular basis
C. Setup a mock video camera next to the special card reader adjacent to the secure door
D. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

**Answer:** B

**NEW QUESTION 83**
- (Topic 1)
You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer.
You are confident that this security implementation will protect the customer from password abuse.
Two months later, a group of hackers called "HackJihad" found a way to access the one- time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.
Your decision of password policy implementation has cost the bank with USD 925, 000 to hackers. You immediately shut down the e-banking website while figuring out the next best
security solution
What effective security solution will you recommend in this case?

A. Implement Biometrics based password authentication syste
B. Record the customers face image to the authentication database
C. Configure your firewall to block logon attempts of more than three wrong tries
D. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
E. Implement RSA SecureID based authentication system

**Answer:** D

**NEW QUESTION 85**

- (Topic 1)
While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

A. The firewall is dropping the packets
B. An in-line IDS is dropping the packets
C. A router is blocking ICMP
D. The host does not respond to ICMP packets

**Answer:** C

**NEW QUESTION 90**
- (Topic 1)
Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to notify administrators of problems or performance.

What default port Syslog daemon listens on?

A. 242
B. 312
C. 416
D. 514

**Answer:** D

**NEW QUESTION 95**
- (Topic 1)
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Port Scanning
B. Single Scanning
C. External Scanning
D. Vulnerability Scanning

**Answer:** D

**NEW QUESTION 99**
- (Topic 1)
Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.
Which of the following commands extracts the HINFO record?

A. Option A
B. Option B
C. Option C
D. Option D

**Answer:** A

**NEW QUESTION 101**
- (Topic 1)
What type of attack is shown in the following diagram?

A. Man-in-the-Middle (MiTM) Attack
B. Session Hijacking Attack
C. SSL Spoofing Attack
D. Identity Stealing Attack

**Answer:** A

**NEW QUESTION 105**
- (Topic 1)
An attacker has successfully compromised a remote computer. Which of the following comes as one of the last steps that should be taken to ensure that the compromise cannot be traced back to the source of the problem?

A. Install patches
B. Setup a backdoor
C. Install a zombie for DDOS
D. Cover your tracks

**Answer:** D

**NEW QUESTION 108**
- (Topic 1)
What is the problem with this ASP script (login.asp)?

A. The ASP script is vulnerable to Cross Site Scripting attack
B. The ASP script is vulnerable to Session Splice attack
C. The ASP script is vulnerable to XSS attack
D. The ASP script is vulnerable to SQL Injection attack

**Answer:** D

**NEW QUESTION 113**
- (Topic 1)
Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area. How would you describe Jason's behavior within a security context?

A. Smooth Talking
B. Swipe Gating
C. Tailgating
D. Trailing

**Answer:** C

**NEW QUESTION 115**
- (Topic 2)
What type of attack is shown here?

A. Bandwidth exhaust Attack
B. Denial of Service Attack
C. Cluster Service Attack
D. Distributed Denial of Service Attack

**Answer:** D

**Explanation:**
We think this is a DDoS attack not DoS because the attack is initialed in multiple zombies not single machine.

**NEW QUESTION 116**
- (Topic 2)
Which of the following encryption is NOT based on block cipher?

A. DES
B. Blowfish
C. AES (Rijndael)
D. RC4

**Answer:** D

**NEW QUESTION 119**
- (Topic 2)
Which port, when configured on a switch receives a copy of every packet that passes through it?

A. R-DUPE Port
B. MIRROR port
C. SPAN port
D. PORTMON

**Answer:** C

**NEW QUESTION 120**
- (Topic 2)
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

**Answer:** C

**NEW QUESTION 125**
- (Topic 2)
Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company's strict security policies that have been implemented, and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two- factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number. Joseph's company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two- factor authentication?

A. Biometric device
B. OTP
C. Proximity cards
D. Security token

**Answer:** D

**NEW QUESTION 130**
- (Topic 2)
While testing web applications, you attempt to insert the following test script into the search area on the company's web site:
<script>alert('Testing Testing Testing')</script>
Later, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

A. Cross Site Scripting
B. Password attacks
C. A Buffer Overflow
D. A hybrid attack

**Answer:** A

**NEW QUESTION 135**
- (Topic 2)
Which definition 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 was 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 that makes it insecure

**Answer:** B

**NEW QUESTION 136**
- (Topic 2)
Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.
Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.
What kind of Denial of Service attack was best illustrated in the scenario above?

A. Simple DDoS attack
B. DoS attacks which involves flooding a network or system
C. DoS attacks which involves crashing a network or system
D. DoS attacks which is done accidentally or deliberately

**Answer:** C

**NEW QUESTION 140**
- (Topic 2)
When writing shellcodes, you must avoid because these will end the string.

A. Root bytes
B. Null bytes
C. Char bytes
D. Unicode bytes

**Answer:** B

**NEW QUESTION 141**
- (Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network. You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
D. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

**Answer:** BD

**NEW QUESTION 143**
- (Topic 2)
LAN Manager Passwords are concatenated to 14 bytes, and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

A. 0xAAD3B435B51404EE
B. 0xAAD3B435B51404AA
C. 0xAAD3B435B51404BB
D. 0xAAD3B435B51404CC

**Answer:** A

**NEW QUESTION 145**
- (Topic 2)
You establish a new Web browser connection to Google. Since a 3-way handshake is required for any TCP connection, the following actions will take place.

? DNS query is sent to the DNS server to resolve www.google.com
? DNS server replies with the IP address for Google?
? SYN packet is sent to Google.
? Google sends back a SYN/ACK packet
? Your computer completes the handshake by sending an ACK
? The connection is established and the transfer of data commences
Which of the following packets represent completion of the 3-way handshake?

A. 4th packet
B. 3rdpacket
C. 6th packet
D. 5th packet

**Answer:** D

**NEW QUESTION 147**
- (Topic 2)
What is the default Password Hash Algorithm used by NTLMv2?

A. MD4
B. DES
C. SHA-1
D. MD5

**Answer:** D

**NEW QUESTION 152**
- (Topic 2)
John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

A. hping2
B. nessus
C. nmap
D. make

**Answer:** B

**NEW QUESTION 153**
- (Topic 2)
Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.
He receives the following SMS message during the weekend.

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's network with the hping command.
Which of the following hping2 command is responsible for the above snort alert?

A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118
B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118
C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118
D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

**Answer:** A

**NEW QUESTION 154**
- (Topic 2)
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

**Explanation:**
ARP poisoning is the closest value to the right answer because ARP spoofing, also known as ARP flooding, ARP poisoning or ARP poison routing (APR), is a technique used to attack a local-area network (LAN). ARP spoofing may allow an attacker to interceptdata frames on a LAN, modify the traffic, or stop the traffic altogether. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP) and not another method of address resolution.

**NEW QUESTION 155**
- (Topic 2)
An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker's fake site shows up and dupes victims by the fake news.

This is another great example that some people do not know what URL's are. Real website:
Fake website: http://www.zuckerjournals.com

The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It's the address that you enter into the address bar at the top your browser and this is clearly not legit site, its www.zuckerjournals.com
How would you verify if a website is authentic or not?

A. Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity
B. Navigate to the site by visiting various blogs and forums for authentic links
C. Enable Cache on your browser and lookout for error message warning on the screen
D. Visit the site by clicking on a link from Google search engine

**Answer:** D

**NEW QUESTION 157**
- (Topic 2)
You are gathering competitive intelligence on an organization. You notice that they have
jobs listed on a few Internet job-hunting sites. There are two jobs for network and system administrators. How can this help you in foot printing the organization?

A. To learn about the IP range used by the target network
B. To identify the number of employees working for the company
C. To test the limits of the corporate security policy enforced in the company
D. To learn about the operating systems, services and applications used on the network

**Answer:** D

**NEW QUESTION 158**
- (Topic 2)
Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet:

How can you protect/fix the problem of your application as shown above?

A. Because the counter starts with 0, we would stop when the counter is less than 200
B. Because the counter starts with 0, we would stop when the counter is more than 200
C. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data
D. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data

**Answer:** AD

**NEW QUESTION 160**
- (Topic 2)
TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

A. SYN flag
B. ACK flag
C. FIN flag
D. XMAS flag

**Answer:** B

**NEW QUESTION 164**
- (Topic 2)
You have successfully gained access to a victim's computer using Windows 2003 Server SMB Vulnerability. Which command will you run to disable auditing from the cmd?

A. stoplog stoplog ?
B. EnterPol /nolog
C. EventViewer o service
D. auditpol.exe /disable

**Answer:** D

**NEW QUESTION 168**
- (Topic 2)
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

A. RST flag scanning
B. FIN flag scanning
C. SYN flag scanning
D. ACK flag scanning

**Answer:** D

**NEW QUESTION 173**
- (Topic 2)
E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.

Select a feature, which you will NOT be able to accomplish with this probe?

A. When the e-mail was received and read
B. Send destructive e-mails
C. GPS location and map of the recipient
D. Time spent on reading the e-mails
E. Whether or not the recipient visited any links sent to them
F. Track PDF and other types of attachments
G. Set messages to expire after specified time
H. Remote control the User's E-mail client application and hijack the traffic

**Answer:** H

**NEW QUESTION 174**
- (Topic 2)
Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company's intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.
What Google search will accomplish this?

A. related:intranet allinurl:intranet:"human resources"
B. cache:"human resources" inurl:intranet(SharePoint)
C. intitle:intranet inurl:intranet+intext:"human resources"
D. site:"human resources"+intext:intranet intitle:intranet

**Answer:** C

**NEW QUESTION 175**
- (Topic 2)
You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

A. Visit Google's search engine and view the cached copy

B. Crawl the entire website and store them into your computer
C. Visit Archive.org web site to retrieve the Internet archive of the company's website
D. Visit the company's partners and customers website for this information

**Answer:** C

**Explanation:**
The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at www.archive.org.

**NEW QUESTION 176**
- (Topic 2)
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

What is the hexadecimal value of NOP instruction?

A. 0x60
B. 0x80
C. 0x70
D. 0x90

**Answer:** D

**NEW QUESTION 180**
- (Topic 2)
Which of the following Trojans would be considered 'Botnet Command Control Center'?

A. YouKill DOOM
B. Damen Rock
C. Poison Ivy
D. Matten Kit

**Answer:** C

**NEW QUESTION 184**
- (Topic 2)
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
B. Attacker floods TCP SYN packets with random source addresses towards a victim host
C. Attacker generates TCP ACK packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host

**Answer:** B

**NEW QUESTION 187**
- (Topic 2)
NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network

printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443
B. 139
C. 179
D. 445

**Answer:** D

**NEW QUESTION 192**
- (Topic 2)
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 150
B. 161
C. 169
D. 69

**Answer:** B

**NEW QUESTION 196**
- (Topic 2)
Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

A. This response means the port he is scanning is open.
B. The RST/ACK response means the port Fred is scanning is disabled.
C. This means the port he is scanning is half open.
D. This means that the port he is scanning on the host is closed.

**Answer:** D

**NEW QUESTION 198**
- (Topic 2)
How do you defend against MAC attacks on a switch?

A. Disable SPAN port on the switch
B. Enable SNMP Trap on the switch
C. Configure IP security on the switch
D. Enable Port Security on the switch

**Answer:** D

**NEW QUESTION 201**
- (Topic 2)
One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a process, then the private key can be derived.

A. Factorization
B. Prime Detection
C. Hashing
D. Brute-forcing

**Answer:** A

**NEW QUESTION 202**
- (Topic 2)
_____ is a type of symmetric-key encryption algorithm that transforms a fixed- length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length.

A. Stream Cipher
B. Block Cipher
C. Bit Cipher
D. Hash Cipher

**Answer:** B

**NEW QUESTION 207**
- (Topic 2)
Gerald, the Systems Administrator for Hyped Enterprises, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, he discovers numerous remote tools were installed that no one claims to have knowledge of in his department. Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to a proxy server in Brazil. Gerald calls the company that owns

the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China. What proxy tool has Gerald's attacker used to cover their tracks?

A. ISA proxy
B. IAS proxy
C. TOR proxy
D. Cheops proxy

**Answer:** C

**NEW QUESTION 211**
- (Topic 2)
What is the command used to create a binary log file using tcpdump?

A. tcpdump -w ./log
B. tcpdump -r log
C. tcpdump -vde logtcpdump -vde ? log
D. tcpdump -l /var/log/

**Answer:** A

**NEW QUESTION 214**
- (Topic 2)
The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

A. 9A.9
B. 17B.17
C. 20C.20
D. 32D.32
E. 35E.35

**Answer:** B

**NEW QUESTION 216**
- (Topic 3)
Which of the following statements are true regarding N-tier architecture? (Choose two.)

A. Each layer must be able to exist on a physically independent system.
B. The N-tier architecture must have at least one logical layer.
C. Each layer should exchange information only with the layers above and below it.
D. When a layer is changed or updated, the other layers must also be recompiled or modified.

**Answer:** AC

**NEW QUESTION 221**
- (Topic 3)
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy
B. Acceptable-use policy
C. Remote-access policy
D. Permissive policy

**Answer:** C

**NEW QUESTION 226**
- (Topic 3)
Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would like to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

A. MD5
B. PGP
C. RSA
D. SSH

**Answer:** D

**NEW QUESTION 229**
- (Topic 3)
Lauren is performing a network audit for her entire company. The entire network is comprised of around 500 computers. Lauren starts an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receives responses from around five hosts. Why did this ping sweep only produce a few responses?

A. Only Windows systems will reply to this scan.
B. A switched network will not respond to packets sent to the broadcast address.
C. Only Linux and Unix-like (Non-Windows) systems will reply to this scan.
D. Only servers will reply to this scan.

**Answer:** C

**NEW QUESTION 230**
- (Topic 3)
Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7? (Select 2 answers)

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run
C. HKEY_CURRENT_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

**Answer:** AD

**NEW QUESTION 235**
- (Topic 3)
You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.
Here is the captured data in tcpdump.
What are the next sequence and acknowledgement numbers that the router will send to the victim machine?

A. Sequence number: 82980070 Acknowledgement number: 17768885A.
B. Sequence number: 17768729 Acknowledgement number: 82980070B.
C. Sequence number: 87000070 Acknowledgement number: 85320085C.
D. Sequence number: 82980010 Acknowledgement number: 17768885D.

**Answer:** A

**NEW QUESTION 238**
- (Topic 3)
John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

A. The hacker is attempting to compromise more machines on the network
B. The hacker is planting a rootkit
C. The hacker is running a buffer overflow exploit to lock down the system
D. The hacker is trying to cover his tracks

**Answer:** D

**NEW QUESTION 239**
- (Topic 3)
Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment
B. Penetration testing
C. Risk assessment
D. Security auditing

**Answer:** D

**NEW QUESTION 240**
- (Topic 3)
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

**Answer:** D

**NEW QUESTION 243**
- (Topic 3)
The GET method should never be used when sensitive data such as credit card is being sent to a CGI program. This is because any GET command will appear in the URL, and will be logged by any servers. For example, let's say that you've entered your credit card information into a form that uses the GET method. The URL may appear like this:
https://www.xsecurity-bank.com/creditcard.asp?cardnumber=453453433532234
The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information. How would you protect from this type of attack?

A. Never include sensitive information in a script
B. Use HTTPS SSLv3 to send the data instead of plain HTTPS
C. Replace the GET with POST method when sending data
D. Encrypt the data before you send using GET method

**Answer:** C

**NEW QUESTION 244**
- (Topic 3)
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.
B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

**Answer:** A

**NEW QUESTION 246**
- (Topic 3)
A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

A. A competitor to the company because they can directly benefit from the publicity generated by making such an attack
B. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants
C. The CEO of the company because he has access to all of the computer systems
D. A government agency since they know the company's computer system strengths and weaknesses

**Answer:** B

**NEW QUESTION 250**
- (Topic 3)
Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

A. Port Security
B. IPSec Encryption
C. Network Admission Control (NAC)
D. 802.1q Port Based Authentication

E. 802.1x Port Based Authentication
F. Intrusion Detection System (IDS)

**Answer:** ACE

**NEW QUESTION 252**
- (Topic 3)
Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

**Answer:** A

**NEW QUESTION 255**
- (Topic 3)
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1
B. MD5
C. HAVAL
D. MD4

**Answer:** A

**NEW QUESTION 258**
- (Topic 3)
The SNMP Read-Only Community String is like a password. The string is sent along with each SNMP Get-Request and allows (or denies) access to a device. Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string". How would you keep intruders from getting sensitive information regarding the network devices using SNMP? (Select 2 answers)

A. Enable SNMPv3 which encrypts username/password authentication
B. Use your company name as the public community string replacing the default 'public'
C. Enable IP filtering to limit access to SNMP device
D. The default configuration provided by device vendors is highly secure and you don't need to change anything

**Answer:** AC

**NEW QUESTION 262**
- (Topic 3)
Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:
HEAD / HTTP/1.0
After pressing enter twice, Blake gets the following results: What has Blake just accomplished?

A. Downloaded a file to his local computer
B. Submitted a remote command to crash the server
C. Poisoned the local DNS cache of the server
D. Grabbed the Operating System banner

**Answer:** D

**NEW QUESTION 264**
- (Topic 3)
Trojan horse attacks pose one of the most serious threats to computer security. The image below shows different ways a Trojan can get into a system. Which are the easiest and most convincing ways to infect a computer?

A. IRC (Internet Relay Chat)
B. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
C. NetBIOS (File Sharing)
D. Downloading files, games and screensavers from Internet sites

**Answer:** B

**NEW QUESTION 268**
- (Topic 3)
What is the broadcast address for the subnet 190.86.168.0/22?

A. 190.86.168.255
B. 190.86.255.255
C. 190.86.171.255
D. 190.86.169.255

**Answer:** C

**NEW QUESTION 273**
- (Topic 3)
Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer's and client's agreement for this particular case. What can Blane use to accomplish this?

A. He can use a split-DNS service to ensure the email is not forwarded on.
B. A service such as HTTrack would accomplish this.
C. Blane could use MetaGoofil tracking tool.
D. Blane can use a service such as ReadNotify tracking tool.

**Answer:** D

**NEW QUESTION 277**
- (Topic 3)
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

**Answer:** A

**NEW QUESTION 282**
- (Topic 3)
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

**Answer:** A

**NEW QUESTION 283**
- (Topic 3)
Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.
John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

What kind of attack did the Hacker attempt to carry out at the bank?

A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
C. The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
D. The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.

**Answer:** D

**NEW QUESTION 287**
- (Topic 3)
If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

A. 31400

B. 31402
C. The zombie will not send a response
D. 31401

**Answer:** B

**Explanation:**
31402 is the correct answer.

**NEW QUESTION 290**
- (Topic 3)
Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to
perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:
SELECT * from Users where username='admin' ?AND password='' AND email like '%@testers.com%'
What will the SQL statement accomplish?

A. If the page is susceptible to SQL injection, it will look in the Users table for usernames of admin
B. This statement will look for users with the name of admin, blank passwords, and email addresses that end in @testers.com
C. This Select SQL statement will log James in if there are any users with NULL passwords
D. James will be able to see if there are any default user accounts in the SQL database

**Answer:** B

**Explanation:**
This query will search for admin user with blank password with mail address @testers.com

**NEW QUESTION 292**
- (Topic 3)
Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

A. Neil has used a tailgating social engineering attack to gain access to the offices
B. He has used a piggybacking technique to gain unauthorized access
C. This type of social engineering attack is called man trapping
D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics

**Answer:** A

**NEW QUESTION 295**
- (Topic 3)
One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator.
B. steganography.
C. a covert channel.
D. asymmetric routing.

**Answer:** C

**NEW QUESTION 297**
- (Topic 3)
You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?

What is the length of the MD5 hash?

A. 32 character
B. 64 byte
C. 48 char
D. 128 kb

**Answer:** A

**NEW QUESTION 300**
- (Topic 3)
Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

A. Hayden is attempting to find live hosts on her company's network by using an XMAS scan
B. She is utilizing a SYN scan to find live hosts that are listening on her network
C. The type of scan, she is using is called a NULL scan
D. Hayden is using a half-open scan to find live hosts on her network

**Answer:** D

**NEW QUESTION 305**
- (Topic 3)
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

**Answer:** C

**NEW QUESTION 308**
- (Topic 3)
SSL has been seen as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

A. SSL is redundant if you already have IDS's in place
B. SSL will trigger rules at regular interval and force the administrator to turn them off
C. SSL will slow down the IDS while it is breaking the encryption to see the packet content
D. SSL will blind the content of the packet and Intrusion Detection Systems will not be able to detect them

**Answer:** D

**NEW QUESTION 312**
- (Topic 3)
A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company's network. Which ports should the administrator open? (Choose three.)

A. Port 22
B. Port 23
C. Port 25
D. Port 53
E. Port 80
F. Port 139
G. Port 445

**Answer:** CDE

**NEW QUESTION 315**
- (Topic 3)
A hacker, who posed as a heating and air conditioning specialist, was able to install a
sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

**Answer:** B

**NEW QUESTION 320**
- (Topic 3)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

**Answer:** D

**Explanation:**
Mole is an automatic SQL Injection exploitation tool. Only by providing a vulnerable URL and a valid string on the site it can detect the injection and exploit it, either by using the union technique or a Boolean query based technique. The Mole uses a command based interface, allowing the user to indicate the action he wants to perform easily

**NEW QUESTION 322**
- (Topic 3)
Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?

A. Jacob is seeing a Smurf attack.
B. Jacob is seeing a SYN flood.
C. He is seeing a SYN/ACK attack.
D. He has found evidence of an ACK flood.

**Answer:** B

**NEW QUESTION 324**
- (Topic 3)
What type of port scan is represented here.

A. Stealth Scan
B. Full Scan
C. XMAS Scan
D. FIN Scan

**Answer:** A

**NEW QUESTION 326**
- (Topic 3)
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

**Answer:** D

**NEW QUESTION 331**
- (Topic 3)
Which of the following represent weak password? (Select 2 answers)

A. Passwords that contain letters, special characters, and numbers Exampl
B. ap1$%##f@52
C. Passwords that contain only numbers Exampl
D. 23698217
E. Passwords that contain only special characters Exampl
F. &*#@!(%)
G. Passwords that contain letters and numbers Exampl
H. meerdfget123
I. Passwords that contain only letters Exampl
J. QWERTYKLRTY
K. Passwords that contain only special characters and numbers Exampl
L. 123@$45
M. Passwords that contain only letters and special characters Exampl
N. bob@&ba
O. Passwords that contain Uppercase/Lowercase from a dictionary list Exampl
P. OrAnGe

**Answer:** EH

**NEW QUESTION 335**
- (Topic 3)
Which of the following are password cracking tools? (Choose three.)

A. BTCrack
B. John the Ripper
C. KerbCrack
D. Nikto
E. Cain and Abel
F. Havij

**Answer:** BCE

**NEW QUESTION 340**
- (Topic 3)
Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in: http://www.youremailhere.com/mail.asp?mailbox=Kevin&Smith=121%22 Kevin changes the URL to: http://www.youremailhere.com/mail.asp?mailbox=Katy&Sanchez=121%22 Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy's mailbox?

A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access
B. By changing the mailbox's name in the URL, Kevin is attempting directory transversal
C. Kevin is trying to utilize query string manipulation to gain access to her email account
D. He is attempting a path-string attack to gain access to her mailbox

**Answer:** C

**NEW QUESTION 344**
- (Topic 3)
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification
B. At least once every three years or after any significant upgrade or modification
C. At least twice a year or after any significant upgrade or modification
D. At least once every two years and after any significant upgrade or modification

**Answer:** A

**NEW QUESTION 348**
- (Topic 3)
What do you call a pre-computed hash?

A. Sun tables
B. Apple tables
C. Rainbow tables
D. Moon tables

**Answer:** C

**NEW QUESTION 353**
- (Topic 3)
Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

**Answer:** A

**NEW QUESTION 356**
- (Topic 3)
Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

**Answer:** D

**NEW QUESTION 359**
- (Topic 3)
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

**Answer:** C

**NEW QUESTION 363**
- (Topic 3)
Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)

A. Alternate between typing the login credentials and typing characters somewhere else in the focus window
B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
D. The next key typed replaces selected text portio
E. E.
F. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"
G. The next key typed replaces selected text portio
H. E.
I. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"

**Answer:** ACDE

**NEW QUESTION 365**
- (Topic 3)
Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

**Answer:** A

**NEW QUESTION 370**
- (Topic 3)
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

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

**Answer:** D

**NEW QUESTION 372**
- (Topic 3)
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

**Answer:** C

**NEW QUESTION 376**
- (Topic 3)
When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one
B. Continues to evaluate the packet until all rules are checked
C. Stops checking rules, sends an alert, and lets the packet continue
D. Blocks the connection with the source IP address in the packet

**Answer:** B

**NEW QUESTION 381**
- (Topic 3)
Here is the ASCII Sheet.

You want to guess the DBO username juggyboy (8 characters) using Blind SQL Injection technique.
What is the correct syntax?

A. Option A
B. Option B
C. Option C
D. Option D

**Answer:** A

**NEW QUESTION 385**
- (Topic 4)
A security analyst in an insurance company is assigned to test a new web application that
will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input fieID.
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"
When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".
Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery
B. Command injection
C. Cross-site scripting
D. SQL injection

**Answer:** C

**NEW QUESTION 387**
- (Topic 4)
Which results will be returned with the following Google search query?
site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting

D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

**Answer:** B

**NEW QUESTION 388**
- (Topic 4)
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Dumper
C. USB Sniffer
D. USB Snoopy

**Answer:** B

**NEW QUESTION 392**
- (Topic 4)
Which of the following parameters enables NMAP's operating system detection feature?

A. NMAP -sV
B. NMAP -oS
C. NMAP -sR
D. NMAP -O

**Answer:** D

**NEW QUESTION 393**
- (Topic 4)
The use of technologies like IPSec can help guarantee the followinG. authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

**Answer:** A

**NEW QUESTION 395**
- (Topic 4)
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

**Answer:** B

**NEW QUESTION 398**
- (Topic 4)
Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis
B. Threat identification, response identification, mitigation identification
C. Attack profile, defense profile, loss profile
D. System profile, vulnerability identification, security determination

**Answer:** A

**NEW QUESTION 403**
- (Topic 4)
Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

**Answer:** C

**NEW QUESTION 404**
- (Topic 4)
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
DatE. Mon, 16 Jan 2011 01:41:33 GMT
Content-TypE. text/html Accept-Ranges: bytes
Last-ModifieD. Wed, 28 Dec 2010 15:32:21 GMT
ETaG. "b0aac0542e25c31:89d" Content-Length: 7369
Which of the following is an example of what the engineer performed?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

**Answer:** B

**NEW QUESTION 408**
- (Topic 4)
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

**Answer:** C

**NEW QUESTION 410**
- (Topic 4)
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Reflective
C. Active
D. Distributive

**Answer:** C

**NEW QUESTION 413**
- (Topic 4)
In keeping with the best practices of layered security, where are the best places to place intrusion detection/intrusion prevention systems? (Choose two.)

A. HID/HIP (Host-based Intrusion Detection/Host-based Intrusion Prevention)
B. NID/NIP (Node-based Intrusion Detection/Node-based Intrusion Prevention)
C. NID/NIP (Network-based Intrusion Detection/Network-based Intrusion Prevention)
D. CID/CIP (Computer-based Intrusion Detection/Computer-based Intrusion Prevention)

**Answer:** AC

**NEW QUESTION 416**
- (Topic 4)
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 the 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:89

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

**Answer:** D

**NEW QUESTION 419**
- (Topic 4)
A hacker was able to sniff packets on a company's wireless network. The following information was discovereD.
The Key 10110010 01001011
The Cyphertext 01100101 01011010
Using the Exlcusive OR, what was the original message?

A. 00101000 11101110

B. 11010111 00010001
C. 00001101 10100100
D. 11110010 01011011

**Answer:** B

**NEW QUESTION 423**
- (Topic 4)
There is a WEP encrypted wireless access point (AP) with no clients connected. In order to crack the WEP key, a fake authentication needs to be performed. What information is needed when performing fake authentication to an AP? (Choose two.)

A. The IP address of the AP
B. The MAC address of the AP
C. The SSID of the wireless network
D. A failed authentication packet

**Answer:** BC

**NEW QUESTION 428**
- (Topic 4)
Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

**Answer:** B

**NEW QUESTION 429**
- (Topic 4)
Which of the following is an example of an asymmetric encryption implementation?

A. SHA1
B. PGP
C. 3DES
D. MD5

**Answer:** B

**NEW QUESTION 431**
- (Topic 4)
Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

**Answer:** C

**NEW QUESTION 432**
- (Topic 4)
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

**Answer:** B

**NEW QUESTION 435**
- (Topic 4)
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

**Answer:** B

**NEW QUESTION 436**
- (Topic 4)

What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25
C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

**Answer:** D

**NEW QUESTION 441**
- (Topic 4)
Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory
B. Discretionary
C. Rule-based
D. Role-based

**Answer:** C

**NEW QUESTION 443**
- (Topic 4)
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

A. Defeating the scanner from detecting any code change at the kernel
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
C. Performing common services for the application process and replacing real applications with fake ones
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

**Answer:** D

**NEW QUESTION 447**
- (Topic 4)
Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

**Answer:** C

**NEW QUESTION 448**
- (Topic 4)
Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

A. Firewall
B. Honeypot
C. Core server
D. Layer 4 switch

**Answer:** B

**NEW QUESTION 450**
- (Topic 4)
How is sniffing broadly categorized?

A. Active and passive
B. Broadcast and unicast
C. Unmanaged and managed
D. Filtered and unfiltered

**Answer:** A

**NEW QUESTION 451**
- (Topic 4)
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

**Answer:** C

**NEW QUESTION 455**
- (Topic 4)
A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:
Untrust (Internet) – (Remote network = 217.77.88.0/24) DMZ (DMZ) – (11.12.13.0/24)
Trust (Intranet) – (192.168.0.0/24)
The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

**Answer:** B

**NEW QUESTION 458**
- (Topic 4)
What is the outcome of the comm”nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

**Answer:** B

**NEW QUESTION 459**
- (Topic 4)
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

**Answer:** B

**NEW QUESTION 460**
- (Topic 4)
If the final set of security controls does not eliminate all risk in a system, what could be done next?

A. Continue to apply controls until there is zero risk.
B. Ignore any remaining risk.
C. If the residual risk is low enough, it can be accepted.
D. Remove current controls since they are not completely effective.

**Answer:** C

**NEW QUESTION 462**
- (Topic 4)
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network’s IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

**Answer:** A

**NEW QUESTION 465**
- (Topic 4)
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

**Answer:** C

**NEW QUESTION 470**
- (Topic 4)
Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature

B. Anomaly
C. Passive
D. Reactive

**Answer:** AB

**NEW QUESTION 475**
- (Topic 4)
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

**Answer:** B

**NEW QUESTION 479**
- (Topic 4)
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

**Answer:** A

**NEW QUESTION 483**
- (Topic 4)
How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

**Answer:** D

**NEW QUESTION 488**
- (Topic 4)
Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Payment Card Industry Data Security Standards (PCI DSS)

**Answer:** D

**NEW QUESTION 493**
- (Topic 4)
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

**Answer:** D

**NEW QUESTION 497**
- (Topic 4)
A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application
B. Layer 4 – TCP
C. Layer 3 – Internet protocol
D. Layer 2 – Data link

**Answer:** B

**NEW QUESTION 500**

- (Topic 4)
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion

**Answer:** D

**NEW QUESTION 503**
- (Topic 4)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

**Answer:** D

**NEW QUESTION 505**
- (Topic 4)
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

**Answer:** B

**NEW QUESTION 506**
- (Topic 4)
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

**Answer:** C

**NEW QUESTION 508**
- (Topic 5)
What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing
B. Secure coding principles
C. Systems security and architecture review
D. Analysis of interrupts within the software

**Answer:** D

**NEW QUESTION 510**
- (Topic 5)
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

**Answer:** A

**NEW QUESTION 511**
- (Topic 5)
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

**Answer:** C

**NEW QUESTION 514**
- (Topic 5)
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

**Answer:** C

**NEW QUESTION 516**
- (Topic 5)
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

**Answer:** A

**NEW QUESTION 519**
- (Topic 5)
Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

**Answer:** C

**NEW QUESTION 524**
- (Topic 5)
What are common signs that a system has been compromised or hacked? (Choose three.)

A. Increased amount of failed logon events
B. Patterns in time gaps in system and/or event logs
C. New user accounts created
D. Consistency in usage baselines
E. Partitions are encrypted
F. Server hard drives become fragmented

**Answer:** ABC

**NEW QUESTION 528**
- (Topic 5)
A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

**Answer:** B

**NEW QUESTION 531**
- (Topic 5)
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

**Answer:** A

**NEW QUESTION 532**
- (Topic 5)
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto

D. hping

**Answer:** A

**NEW QUESTION 535**
- (Topic 5)
Which security control role does encryption meet?

A. Preventative
B. Detective
C. Offensive
D. Defensive

**Answer:** A

**NEW QUESTION 538**
- (Topic 5)
The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

**Answer:** B

**NEW QUESTION 543**
- (Topic 5)
Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher

**Answer:** D

**NEW QUESTION 544**
- (Topic 5)
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. "

**Answer:** A

**NEW QUESTION 547**
- (Topic 5)
Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity
B. Key discovery
C. Bulk data encryption

D. Key recovery

**Answer:** C

**NEW QUESTION 548**
- (Topic 5)
Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

**Answer:** A

**NEW QUESTION 552**
- (Topic 5)
Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis
B. They must be dual-homed
C. Similar RAM requirements
D. Fast network interface cards

**Answer:** B

**NEW QUESTION 555**
- (Topic 5)
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto
C. Ike-scan
D. Arp-scan

**Answer:** C

**NEW QUESTION 557**
- (Topic 5)
An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access
B. Weak SSL version
C. Cleartext login
D. Web portal data leak

**Answer:** A

**NEW QUESTION 559**
- (Topic 5)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

**Answer:** C

**NEW QUESTION 563**
- (Topic 5)
A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. Email server certificate

**Answer:** B

**NEW QUESTION 566**
- (Topic 5)
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

**Answer:** D

**NEW QUESTION 570**
- (Topic 5)
A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.
During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.
Which of the following is an issue with the situation?

A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

**Answer:** A

**NEW QUESTION 572**
- (Topic 5)
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results? TCP port 21 – no response TCP port 22 – no response TCP port 23 – Time-to-live
exceeded

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering devic
D. This indicates that port 23 was not blocked at the firewall.
E. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

**Answer:** C

**NEW QUESTION 575**
- (Topic 5)
Which of the following is a component of a risk assessment?

A. Physical security
B. Administrative safeguards
C. DMZ
D. Logical interface

**Answer:** B

**NEW QUESTION 580**
- (Topic 5)
A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing
B. MAC duplication
C. MAC flooding
D. SYN flood
E. Reverse smurf attack
F. ARP broadcasting

**Answer:** ABC

**NEW QUESTION 583**
- (Topic 5)
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

A. Ping of death
B. SYN flooding
C. TCP hijacking
D. Smurf attack

**Answer:** A

**NEW QUESTION 586**
- (Topic 5)
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 corporate network. What tool should the analyst use to perform a Blackjacking attack?

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

**Answer:** B

**NEW QUESTION 589**
- (Topic 5)
Which of the following open source tools would be the best choice to scan a network for potential targets?

A. NMAP
B. NIKTO
C. CAIN
D. John the Ripper

**Answer:** A

**NEW QUESTION 593**
- (Topic 5)
Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl
B. C++
C. Python
D. Java

**Answer:** B

**NEW QUESTION 594**
- (Topic 5)
Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

A. Smurf attack
B. Social engineering attack
C. SQL injection attack
D. Phishing attack
E. Fraggle attack
F. Distributed denial of service attack

**Answer:** BD

**NEW QUESTION 599**
- (Topic 5)
Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

**Answer:** C

**NEW QUESTION 603**
- (Topic 5)
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

**Answer:** A

**NEW QUESTION 605**
- (Topic 5)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

**Answer:** A

**NEW QUESTION 606**
- (Topic 5)
A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config
D. Ipconfig firewall show config

**Answer:** A

**NEW QUESTION 609**
- (Topic 5)
An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

A. Start by foot printing the network and mapping out a plan of attack.
B. Ask the employer for authorization to perform the work outside the company.
C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

**Answer:** B

**NEW QUESTION 611**
- (Topic 5)
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

**Answer:** D

**NEW QUESTION 615**
- (Topic 5)
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

**Answer:** A

**NEW QUESTION 617**
- (Topic 5)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate,
then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

**Answer:** B

**NEW QUESTION 622**
- (Topic 5)
A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions.
On further research, the tester come across a perl script that runs the following msadc functions:system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");

Which exploit is indicated by this script?

A. A buffer overflow exploit
B. A chained exploit
C. A SQL injection exploit
D. A denial of service exploit

**Answer:** B

**NEW QUESTION 623**
- (Topic 5)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

**Answer:** A

**NEW QUESTION 625**
- (Topic 5)
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

**Answer:** A

**NEW QUESTION 627**
- (Topic 5)
What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

**Answer:** A

**NEW QUESTION 630**
- (Topic 5)
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

**Answer:** A

**NEW QUESTION 634**
- (Topic 5)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

**Answer:** A

**NEW QUESTION 638**
- (Topic 5)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

**Answer:** D

**NEW QUESTION 640**
- (Topic 5)
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.

B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
D. Certain operating systems and adapters do not collect the management or control packets.

**Answer:** D

**NEW QUESTION 645**
- (Topic 5)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

**Answer:** A

**NEW QUESTION 648**
- (Topic 5)
Which of the following are advantages of adopting a Single Sign On (SSO) system? (Choose two.)

A. A reduction in password fatigue for users because they do not need to know multiple passwords when accessing multiple applications
B. A reduction in network and application monitoring since all recording will be completed at the SSO system
C. A reduction in system administration overhead since any user login problems can be resolved at the SSO system
D. A reduction in overall risk to the system since network and application attacks can only happen at the SSO point

**Answer:** AC

**NEW QUESTION 649**
- (Topic 5)
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book
B. ISO 26029
C. Common Criteria
D. The Wassenaar Agreement

**Answer:** C

**NEW QUESTION 653**
- (Topic 5)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

**Answer:** A

**NEW QUESTION 654**
- (Topic 5)
When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the Source IP address and Destination IP address are the same. There have been no alerts sent via email or logged in the IDS. Which type of an alert is this?

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

**Answer:** B

**NEW QUESTION 657**
- (Topic 6)
To what does “message repudiation” refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.
B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
E. Message repudiation means a sender can claim they did not actually send a particular message.

**Answer:** E

**Explanation:**

A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.
Non-repudiation is the opposite quality—a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation – Denial of message submission or delivery.

**NEW QUESTION 662**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CEH-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CEH-001 Product From:

**https://www.2passeasy.com/dumps/CEH-001/**

## Money Back Guarantee

## CEH-001 Practice Exam Features:

* CEH-001 Questions and Answers Updated Frequently

* CEH-001 Practice Questions Verified by Expert Senior Certified Staff

* CEH-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CEH-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year