EC-COUNCIL.312-50v10.v2022-09-05.q240

Exam Code:	312-50v10
Exam Name:	Certified Ethical Hacker Exam (CEH v10)
Certification Provider:	EC-COUNCIL
Free Question Number:	240
Version:	v2022-09-05
# of views:	3270
# of Questions views:	2400
https://www.freepdfdumps.com/EC-COUNCIL.312-50v10.v2022-09-05.q240.html	

NEW QUESTION: 1
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?
A. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
B. Vulnerabilities in the application layer are greatly different from IPv4.
C. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
D. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company.
The phishing message will often use the name of the company CEO, president, or managers. The time a hacker spends performing research to locate this information about a company is known as?
A. Enumeration
B. Investigation
C. Exploration
D. Reconnaissance
Answer: (SHOW ANSWER)

NEW QUESTION: 3
You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address

was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?
A. IDS log
B. Internet Firewall/Proxy log
C. Event logs on domain controller
D. Event logs on the PC
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?
A. Containment phase
B. Recovery phase
C. Identification phase
D. Preparation phase
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
At a Windows Server command prompt, which command could be used to list the running services?
A. Sc config
B. Sc query type= running
C. Sc query
D. Sc query \\servername
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results?
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
A. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
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 device. This indicates that port 23 was not blocked at the firewall
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?
A. SYN flooding
B. TCP hijacking
C. Ping of death
D. Smurf attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Assume a business-crucial web-site of some company that is used to sell handsets to the customers
worldwide. All the developed components are reviewed by the security team on a monthly basis. In order
to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The
tools are written in JavaScript and can track the customer's activity on the site. These tools are located on
the servers of the marketing company.
What is the main security risk associated with this scenario?
A. There is no risk at all as the marketing services are trustworthy
B. External scripts have direct access to the company servers and can steal the data from there
C. External scripts increase the outbound company data traffic which leads greater financial losses
D. External script contents could be maliciously modified without the security team knowledge
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
The "gray box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.
Answer: A (LEAVE A REPLY)
Explanation
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION: 10
Fingerprinting VPN firewalls is possible with which of the following tools?
A. Arp-scan
B. Angry IP
C. Nikto
D. Ike-scan
Answer: D (LEAVE A REPLY)

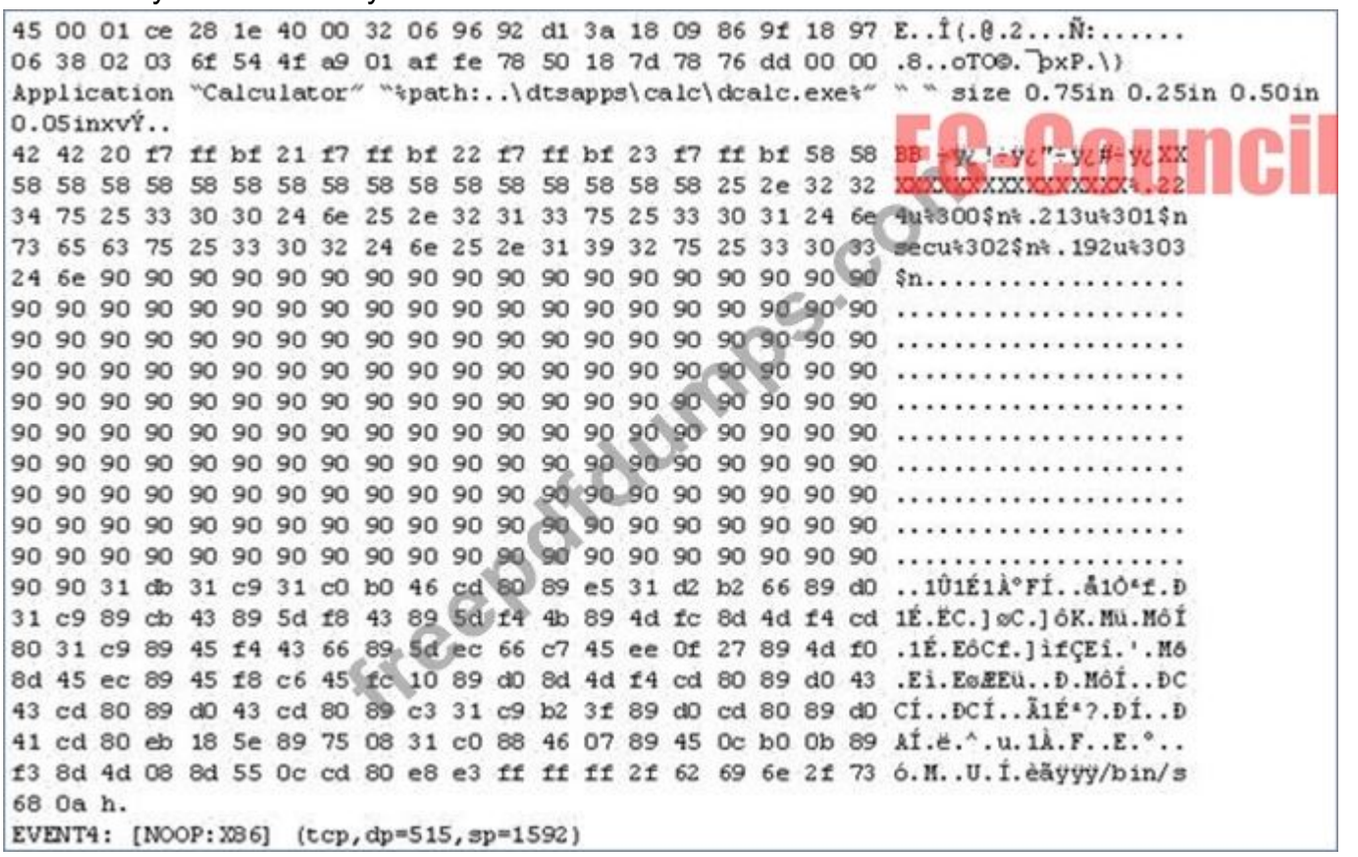
NEW QUESTION: 11
Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make
$1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks
that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content
or UPL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
A. Clickjacking Attack
B. HTTP Parameter Pollution
C. Session Fixation
D. HTML Injection
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?
A. Scripting languages are hard to learn.
B. Scripting languages are not object-oriented.
C. Scripting languages cannot be used to create graphical user interfaces.
D. Scripting languages are slower because they require an interpreter to run the code.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.

You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?



A. The attacker is attempting an exploit that launches a command-line shell

B. The buffer overflow attack has been neutralized by the IDS

C. The attacker is attempting a buffer overflow attack and has succeeded

D. The attacker is creating a directory on the compromised machine

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Scanning

B. System Hacking

C. Enumeration

D. Footprinting

Answer: (SHOW ANSWER)

NEW QUESTION: 15

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability
C. SQL injection vulnerability
D. Web site defacement vulnerability
Answer: A (LEAVE A REPLY)
Explanation
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION: 16
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. Snort
C. John the Ripper
D. Dsniff
Answer: A (LEAVE A REPLY)
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

NEW QUESTION: 17
Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication; which option below offers that?
A. A new username and password
B. His username and a stronger password
C. A fingerprint scanner and his username and password
D. Disable his username and use just a fingerprint scanner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?
A. Disconnect the email server from the network
B. Leave it as it Is and contact the incident response te3m right away
C. Block the connection to the suspicious IP Address from the firewall
D. Migrate the connection to the backup email server
Answer: (SHOW ANSWER)

NEW QUESTION: 19
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?
A. smtp port
B. tcp.port eq 25
C. request smtp 25
D. tcp.contains port 25
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can be used to perform session splicing attacks?
A. Whisker
B. tcpsplice
C. Burp
D. Hydra
Answer: A (LEAVE A REPLY)

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
References:
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

NEW QUESTION: 21
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?
A. Dictionary Attack
B. Online Attack
C. Brute Force Attack
D. Hybrid Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?
A. Private
B. Public
C. Shared
D. Root
Answer: A (LEAVE A REPLY)
Explanation
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.
An attack may also reveal private keys of compromised parties.
References: https://en.wikipedia.org/wiki/Heartbleed

NEW QUESTION: 23
You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.
You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.
In other words, you are trying to penetrate an otherwise impenetrable system.
How would you proceed?
A. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
B. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
C. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly- paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques
Answer: (SHOW ANSWER)

NEW QUESTION: 24
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?
A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -r 10.10.1.0/24
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?
A. Metasploit
B. Wireshark
C. Maltego
D. Nessus
Answer: (SHOW ANSWER)

NEW QUESTION: 26

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?
A. Social engineering
B. Tailgating
C. Piggybacking
D. Eavesdropping
Answer: A (LEAVE A REPLY)
Explanation
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION: 27
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?
A. Disable IPTables
B. Create User Account
C. Download and Install Netcat
D. Disable Key Services
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?
A. Enumeration
B. Reconnaissance
C. Escalation
D. Scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 29

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. is-d abccorp.local

B. List domain=Abccorp.local type=zone

C. list server=192.168.10.2 type=all

D. lserver 192.168.10.2-t all

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

Which of the following will perform an Xmas scan using NMAP?

A. nmap -sV 192.168.1.254

B. nmap -sP 192.168.1.254

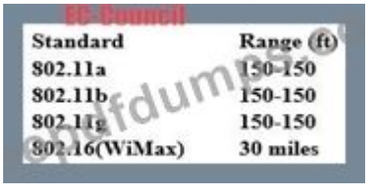
C. nmap -sA 192.168.1.254

D. nmap -sX 192.168.1.254

Answer: (SHOW ANSWER)

NEW QUESTION: 31

From the following table, identify the wrong answer in terms of Range (ft).



A. 802.11b

B. 802.11a

C. 802.11g

D. 802.16(WiMax)

Answer: B (LEAVE A REPLY)

NEW QUESTION: 32

Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA

B. When a secondary name server has had its service restarted

C. When the TTL falls to zero

D. When a primary name server has had its service restarted

E. When a secondary SOA is higher that a primary SOA

Answer: A (LEAVE A REPLY)

NEW QUESTION: 33

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Delete the files and try to determine the source

B. Reload from known good media

C. Reload from a previous backup

D. Perform a trap and trace

E. Copy the system files from a known good system

Answer: (SHOW ANSWER)

NEW QUESTION: 34

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories:

lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Dictionary Attack

B. Online Attack

C. Brute Force Attack

D. Hybrid Attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35

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. 11110010 01011011

B. 00001101 10100100
C. 11010111 00010001
D. 00101000 11101110
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?
A. Running a network scan to detect network services in the corporate DMZ
B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Using configuration management to determine when and where to apply security patches
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Emil uses nmap to scan two hosts using this command.
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?
A. Host 192.168.99.1 is the host that he launched the scan from.
B. Host 192.168.99.7 is an iPad.
C. Host 192.168.99.7 is down.
D. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Cross-site request forgery involves:
A. Modification of a request by a proxy between client and server

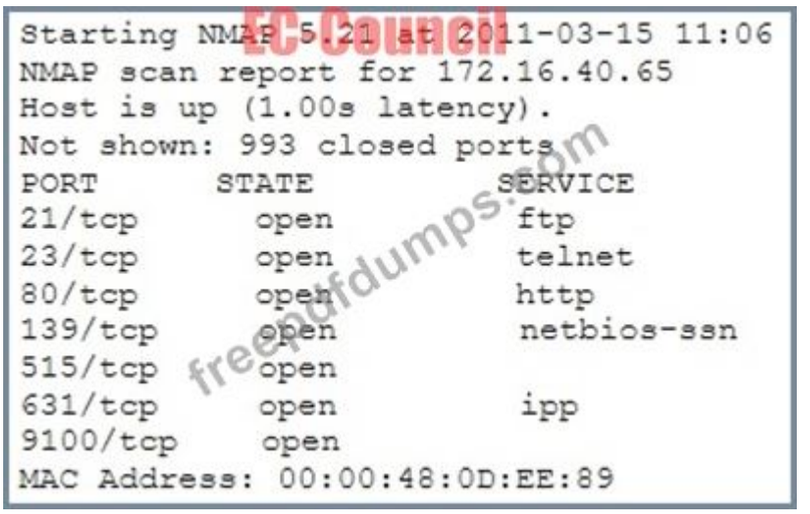
B. A browser making a request to a server without the user's knowledge
C. A request sent by a malicious user from a browser to a server
D. A server making a request to another server without the user's knowledge
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?
A. This is a scam because Bob does not know Scott.
B. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
D. This is probably a legitimate message as it comes from a respectable organization.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
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: (SHOW ANSWER)

NEW QUESTION: 41
What is attempting an injection attack on a web server based on responses to True/False questions called?
A. Compound SQLi
B. DMS-specific SQLi
C. Blind SQLi
D. Classic SQLi
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
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?



A. The host is likely a printer.

B. The host is likely a Windows machine.

C. The host is likely a Linux machine.

D. The host is likely a router.

Answer: (SHOW ANSWER)

Explanation

The Internet Printing Protocol (IPP) uses port 631.

References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 43

Which of the following is a component of a risk assessment?

A. Administrative safeguards

B. Physical security

C. DMZ

D. Logical interface

Answer: A (LEAVE A REPLY)

Risk assessment include:

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

NEW QUESTION: 44

Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Degauss the backup tapes and transport them in a lock box.

B. Encrypt the backup tapes and transport them in a lock box

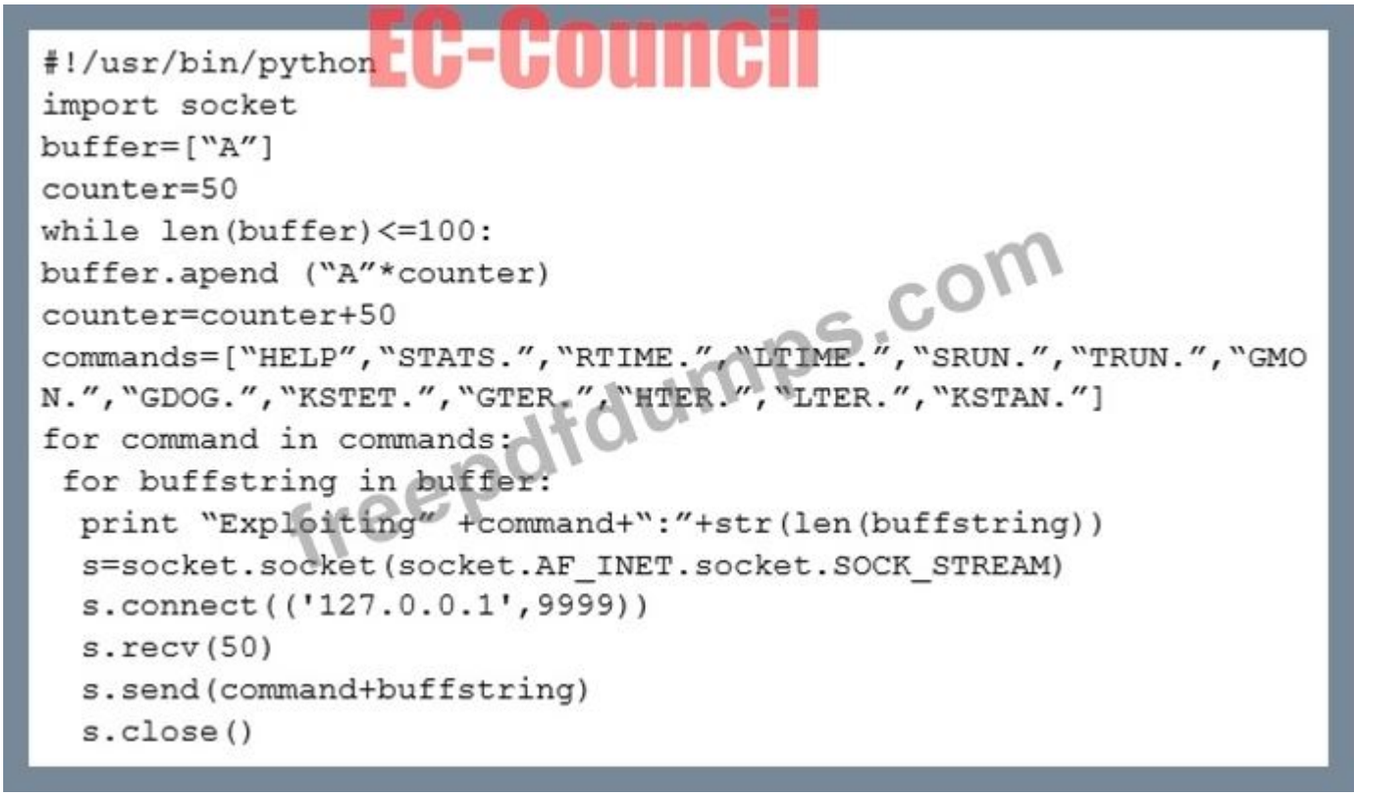
C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Answer: (SHOW ANSWER)

NEW QUESTION: 45

What is the code written for?



A. Encryption

B. Denial-of-service (Dos)

C. Bruteforce

D. Buffer Overflow

Answer: D (LEAVE A REPLY)

NEW QUESTION: 46

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A. Service Oriented Architecture

B. Object Oriented Architecture

C. Lean Coding

D. Agile Process

Answer: (SHOW ANSWER)

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

NEW QUESTION: 47
Which command can be used to show the current TCP/IP connections?
A. Net use
B. Net use connection
C. Netstat
D. Netsh
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following can the administrator do to verify that a tape backup can be recovered in its
entirety?
A. Perform a full restore
B. Read the last 512 bytes of the tape
C. Read the first 512 bytes of the tape
D. Restore a random file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as
realistic as possible; therefore, they did not provide any information besides the company name. What
should be the first step in security testing the client?
A. Reconnaissance
B. Scanning
C. Enumeration
D. Escalation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank.

Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

A. This is scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

B. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.

C. This is probably a legitimate message as it comes from a respectable organization.

D. This is scam because Bob does not know Scott.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 51

Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Scanning

B. Enumeration

C. Social Engineering

D. Sniffing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 52

Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name. What should be the first step in security testing the client?

A. Scanning

B. Reconnaissance

C. Escalation

D. Enumeration

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

A person approaches a network administrator and wants advice on how to send encrypted email from home.

The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)

B. Multipurpose Internet Mail Extensions (MIME)

C. Pretty Good Privacy (PGP)

D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Answer: (SHOW ANSWER)

NEW QUESTION: 54

An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?
A. Chosen ciphertext attack
B. Plaintext attack
C. Meet in the middle attack
D. Birthday attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?
A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24
Answer: A (LEAVE A REPLY)
command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

NEW QUESTION: 56
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. LOGIN, USER
B. USER, PASS
C. USER, NICK
D. LOGIN, NICK
Answer: (SHOW ANSWER)

NEW QUESTION: 57
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?
A. The key entered is based on the Diffie-Hellman method.
B. The key is an RSA key used to encrypt the wireless data.
C. The key entered is a symmetric key used to encrypt the wireless data.
D. The key entered is a hash that is used to prove the integrity of the wireless data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

A. Session hijacking

B. Firewalking

C. Man-in-the middle attack

D. Network sniffing

Answer: B (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 59

Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"".

Which statement below is true?

A. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.

B. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

C. This is a scam because Bob does not know Scott.

D. This is probably a legitimate message as it comes from a respectable organization.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 60

You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.

What may be the problem?

A. Traffic is Blocked on UDP Port 80

B. Traffic is Blocked on UDP Port 53

C. Traffic is Blocked on TCP Port 54

D. Traffic is Blocked on TCP Port 80

Answer: B (LEAVE A REPLY)

NEW QUESTION: 61

A large mobile telephony and data network operator has a data center that houses network elements.

These are essentially large computers running on Linux. The perimeter of the data center is secured with

firewalls and IPS systems.

What is the best security policy concerning this setup?

A. As long as the physical access to the network elements is restricted, there is no need for additional
measures.
B. The operator knows that attacks and down time are inevitable and should have a backup site.
C. Network elements must be hardened with user ids and strong passwords. Regular security tests and
audits should be performed.
D. There is no need for specific security measures on the network elements as long as firewalls and IPS
systems exist.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
Perspective clients want to see sample reports from previous penetration tests.
What should you do next?
A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.
Answer: A (LEAVE A REPLY)
Penetration tests data should not be disclosed to third parties.

NEW QUESTION: 63
You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs. - 192.168.8.0/24. What command you would use?
A. wireshark -fetch "192.168.8/*"
B. tshark -net 192.255.255.255 mask 192.168.8.0
C. sudo tshark -f "net 192.168.8.0/24"
D. wireshark -capture -local -masked 192.168.8.0 -range 24
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?
A. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors
B. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
C. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
D. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
Answer: (SHOW ANSWER)

NEW QUESTION: 65
What is correct about digital signatures?
A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 66
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?
A. Display passwd content to prompt
B. Removes the passwd file
C. Changes all passwords in passwd
D. Add new user to the passwd file
Answer: A (LEAVE A REPLY)
Explanation
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:
() {:;}; /bin/cat /etc/passwd
That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.
References: https://blog.cloudflare.com/inside-shellshock/

NEW QUESTION: 67

If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Idle scan

B. TCP SYN

C. Spoof Scan

D. TCP Connect scan

Answer: B (LEAVE A REPLY)

NEW QUESTION: 68

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to

VHF and UHF?

A. Yagi antenna

B. Dipole antenna

C. Omnidirectional antenna

D. Parabolic grid antenna

Answer: (SHOW ANSWER)

NEW QUESTION: 69

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");
}
```


Output:

Segmentation fault

A. C++

B. Python

C. Java

D. C#

Answer: A (LEAVE A REPLY)

NEW QUESTION: 70

Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.

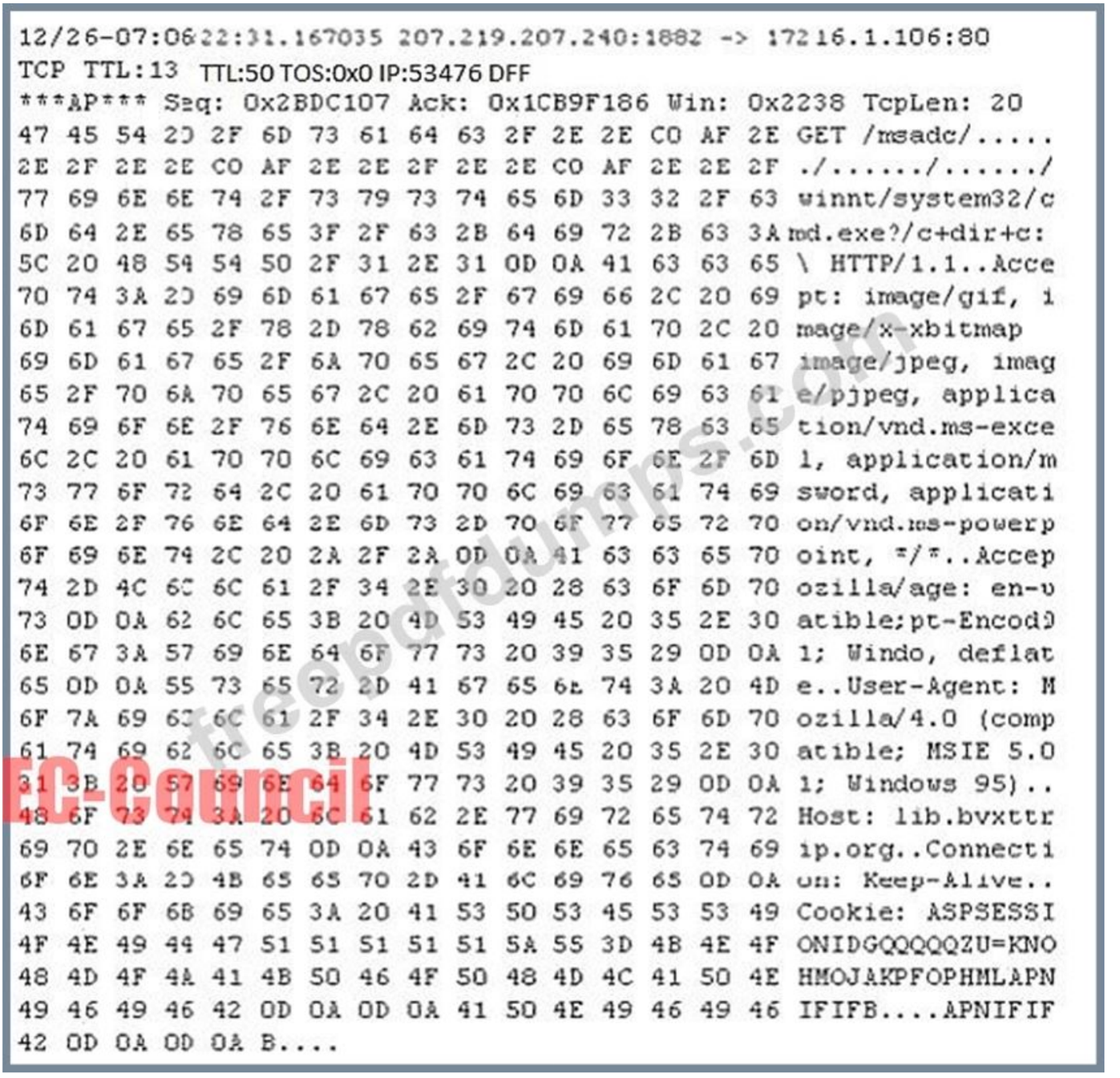
Which of the following activities should not be included in this phase? (see exhibit) Exhibit:

A. III
B. IV
C. III and IV
D. All should be included.
Answer: A (LEAVE A REPLY)
The post-attack phase revolves around returning any modified system(s) to the pretest state.
Examples of such activities:
References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

NEW QUESTION: 71
What is the purpose of DNS AAAA record?
A. Address database record
B. IPv6 address resolution record
C. Authorization, Authentication and Auditing record
D. Address prefix record
Answer: B (LEAVE A REPLY)

NEW QUESTION: 72
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit
Answer: A (LEAVE A REPLY)
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION: 73
Study the following log extract and identify the attack.



A. Hexcode Attack

B. Cross Site Scripting

C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

A. Copy the data to removable media and keep it in case you need it

B. Immediately stop work and contact the proper legal authorities

C. Ignore the data and continue the assessment until completed as agreed
D. Confront the client in a respectful manner and ask her about the data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
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:

Which of the following is an example of what the engineer performed?
A. Cross-site scripting
B. SQL injection
C. Whois database query
D. Banner grabbing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment.
A. Cloud based
B. Heuristics based
C. Honypot based
D. Behavioral based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
PGP, SSL, and IKE are all examples of which type of cryptography?
A. Public Key
B. Secret Key
C. Hash Algorithm
D. Digest
Answer: A (LEAVE A REPLY)
Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL),Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.
References: https://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION: 78
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 lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
B. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
C. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.
D. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following is assured by the use of a hash?
A. Authentication
B. Confidentially
C. Availability
D. Integrity
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 80
What is the purpose of a demilitarized zone on a network?
A. To contain the network devices you wish to protect

B. To scan all traffic coming through the DMZ to the internal network
C. To only provide direct access to the nodes within the DMZ and protect the network behind it
D. To provide a place to put the honeypot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
This kind of password cracking method uses word lists in combination with numbers and special characters:
A. Hybrid
B. Symmetric
C. Linear
D. Brute Force
Answer: (SHOW ANSWER)

NEW QUESTION: 82
How does an operating system protect the passwords used for account logins?
A. The operating system stores all passwords in a protected segment of non-volatile memory.
B. The operating system performs a one-way hash of the passwords.
C. The operating system stores the passwords in a secret file that users cannot find.
D. The operating system encrypts the passwords, and decrypts them when needed.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?
A. The port will send an ACK
B. The port will send a SYN
C. The port will ignore the packets
D. The port will send an RST
Answer: C (LEAVE A REPLY)
Explanation: References:

NEW QUESTION: 84
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?
A. Black Hat
B. Suicide Hacker
C. White Hat
D. Gray Hat

Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
A. 200303028
B. 60
C. 4800
D. 2400
E. 3600
F. 604800
Answer: D (LEAVE A REPLY)

NEW QUESTION: 86
The establishment of a TCP connection involves a negotiation called three-way handshake.
What type of message does the client send to the server in order to begin this negotiation?
A. SYN
B. RST
C. SYN-ACK
D. ACK
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.
Which of the following organizations is being described?
A. Payment Card Industry (PCI)
B. Center for Disease Control (CDC)
C. Institute of Electrical and Electronics Engineers (IEEE)
D. International Security Industry Organization (ISIO)
Answer: (SHOW ANSWER)
Explanation
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).
References: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION: 88
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
A. Nmap
B. Metasploit
C. Nikto
D. Armitage
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.
Which of the following terms best matches the definition?
A. Ransomware
B. Adware
C. Spyware
D. Riskware
Answer: A (LEAVE A REPLY)
Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.
References: https://en.wikipedia.org/wiki/Ransomware

NEW QUESTION: 90
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?
A. Masquerading
B. Tailgating
C. Phishing
D. Whaling

Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 91
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?
A. Host-based intrusion detection system (HIDS)
B. Honeypots
C. Firewalls
D. Network-based intrusion detection system (NIDS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?
A. Analyzing service response
B. Injecting arbitrary data
C. Port scanning
D. Banner grabbing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?
A. iBoot Exploit
B. Bootrom Exploit
C. Userland Exploit
D. Sandbox Exploit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94

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

Dear valued customers,

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

or you may contact us at the following address:

Media Internet Consultants, Edif. Neptuno, Planta

Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

A. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

B. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site

C. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

D. Connect to the site using SSL, if you are successful then the website is genuine

E. Look at the website design, if it looks professional then it is a Real Anti-Virus website

Answer: B (LEAVE A REPLY)

NEW QUESTION: 95

An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

A. The sequence does not matter. Both steps have to be performed against all hosts.

B. The port scan alone is adequate. This way he saves time.

C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.

D. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 96

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security

assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects
both the organization's interest and your liabilities as a tester?
A. Project Scope
B. Rules of Engagement
C. Service Level Agreement
D. Non-Disclosure Agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:
According to the section from the report, which of the following choice is true?
A. There is access control policy between VLANs.
B. Possibility of SQL Injection attack is eliminated.
C. A stateful firewall can be used between intranet (LAN) and DMZ.
D. MAC Spoof attacks cannot be performed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Which of the following is the BEST way to defend against network sniffing?
A. Use Static IP Address
B. Restrict Physical Access to Server Rooms hosting Critical Servers
C. Register all machines MAC Address in a Centralized Database
D. Using encryption protocols to secure network communications
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system whose credentials are known. It was written by sysinternals and has been integrated within the framework. The penetration testers successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is used in the psexec module's 'smbpass' option?
A. LM:NTLM

B. NT:LM
C. NTLM:LM
D. LM:NT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?
A. HIPAA
B. ISO/IEC 27002
C. COBIT
D. FISMA
Answer: A (LEAVE A REPLY)
Explanation
The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by
"covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".
References:
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

NEW QUESTION: 101
_____ is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.
A. DNSSEC
B. Zone transfer
C. Resource transfer
D. Resource records
Answer: (SHOW ANSWER)

NEW QUESTION: 102
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address

B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

Answer: A (LEAVE A REPLY)

Explanation

MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

References: https://en.wikipedia.org/wiki/MAC_filtering

NEW QUESTION: 103

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. MD4

B. HAVAL

C. MD5

D. SHA-1

Answer: D (LEAVE A REPLY)

NEW QUESTION: 104

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. Hping2 cannot be used for idle scanning.

B. These ports are actually open on the target system.

C. A stateful inspection firewall is resetting your queries.

D. The zombie you are using is not truly idle.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 105

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

A. >host -t ns hackeddomain.com

B. >host -t AXFR hackeddomain.com

C. >host -t soa hackeddomain.com

D. >host -t a hackeddomain.com

Answer: D (LEAVE A REPLY)

NEW QUESTION: 106

Which of the following is not a Bluetooth attack?

A. Bluesnarfing
B. Bluedriving
C. Bluesmacking
D. Bluejacking
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 107
Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file named
"Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating,
"This word document is corrupt". In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.
What type of malware has Jesse encountered?
A. Key-Logger
B. Worm
C. Macro Virus
D. Trojan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
A security administrator notices that the log file of the company's webserver contains suspicious entries:

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. LDAP injection.

B. command injection.

C. directory traversal.

D. SQL injection.

Answer: (SHOW ANSWER)

NEW QUESTION: 109

Which of the following items is unique to the N-tier architecture method of designing software applications?

A. It is compatible with various databases including Access, Oracle, and SQL.

B. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.

C. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

D. Application layers can be separated, allowing each layer to be upgraded independently from other layers.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 110

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and

Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible

breach of security. When the investigator attempts to correlate the information in all of the logs, the

sequence of many of the logged events do not match up.

What is the most likely cause?

A. Proper chain of custody was not observed while collecting the logs.

B. The network devices are not all synchronized.
C. The security breach was a false positive.
D. The attacker altered or erased events from the logs.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a ____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.
A. Simple, Complex
B. Strict, Abstract
C. Relational, Hierarchical
D. Hierarchical, Relational
Answer: (SHOW ANSWER)

NEW QUESTION: 112
You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will
run the capture against a specific set of IPs. - 192.168.8.0/24. What command you would use?
A. wireshark -fetch "192.168.8/*"
B. sudo tshark -f "net 192.168.8.0/24"
C. wireshark -capture -local -masked 192.168.8.0 -range 24
D. tshark -net 192.255.255.255 mask 192.168.8.0
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
A. URL Traversal attack
B. SQL Injection
C. Cross-site-scripting attack
D. Buffer Overflow attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information

security such as data confidentially, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Basic example to understand how cryptography works is given below:

SECURE (plain text)
+1 (+1 next letter.for example , the letter""T"" is used for "S" to encrypt.)
TFDVSF (encrypted text)
+=logic=>Algorithm
1=Factor=>Key

Which of the following choices true about cryptography?

A. Algorithm is not the secret; key is the secret.

B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.

C. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.

D. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Answer: C (LEAVE A REPLY)

Explanation

NEW QUESTION: 115

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

What kind of Web application vulnerability likely exists in their software?

A. Defense in depth

B. Security through obscurity

C. Host-Based Intrusion Detection System

D. Network-Based Intrusion Detection System

Answer: A (LEAVE A REPLY)

NEW QUESTION: 116

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

A. Gateway-based IDS

B. Open source-based

C. Host-based IDS

D. Network-based IDS

Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. NetCat
B. Cain and Abel
C. DataThief
D. SQLInjector
Answer: (SHOW ANSWER)

NEW QUESTION: 118
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible?
(Choose two.)
A. It used TCP as the underlying protocol.
B. It is susceptible to sniffing.
C. It is used by all network devices on the market.
D. It uses community string that is transmitted in clear text.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 119
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 (LEAVE A REPLY)
Explanation
A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.
References: https://en.wikipedia.org/wiki/Macro_virus

NEW QUESTION: 120
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering

information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient input validation

B. Insufficient exception handling

C. Insufficient database hardening

D. Insufficient security management

Answer: (SHOW ANSWER)

Explanation

The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

NEW QUESTION: 121

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

A. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

B. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF

C. Switch then acts as hub by broadcasting packets to all machines on the network

D. The CAM overflow table will cause the switch to crash causing Denial of Service

Answer: (SHOW ANSWER)

NEW QUESTION: 122
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch
(.bat) or PowerShell (.ps1) script?
A. Windows firewall
B. Data Execution Prevention (DEP)
C. Address Space Layout Randomization (ASLR)
D. User Access Control (UAC)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?
A. The file reveals the passwords to the root user only.
B. He can open it and read the user ids and corresponding passwords.
C. He cannot read it because it is encrypted.
D. The password file does not contain the passwords themselves.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
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 217.77.88.0/24 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.50 RDP 3389
D. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
A. Private key
B. Hash value

C. Digital certificate
D. Digital signature
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?
A. Locate type=ns
B. Set type=ns
C. Transfer type=ns
D. Request type=ns
Answer: B (LEAVE A REPLY)

NEW QUESTION: 127
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?
A. http enum
B. http-git
C. http-methods
D. http-headers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?
A. NoSQL injection
B. Error-based SQL injection
C. Blind SQL injection
D. Union-based SQL injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?
A. >host -t a hackeddomain.com

B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com
Answer: A (LEAVE A REPLY)
Explanation
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

NEW QUESTION: 130
Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
C. Assigns values to risk probabilities; Impact values.
D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining
A. financial soundness and business viability metrics.
B. contract agreement writing standards.
C. guidelines and practices for security controls.
D. standard best practice for configuration management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 132
A virus that attempts to install itself inside the file it is infecting is called?
A. Tunneling virus
B. Cavity virus
C. Polymorphic virus
D. Stealth virus
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 133
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?
A. User Access Control (UAC)
B. Data Execution Prevention (DEP)
C. Windows firewall

D. Address Space Layout Randomization (ASLR)
Answer: (SHOW ANSWER)

NEW QUESTION: 134
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?
A. SYN Flood
B. SSH
C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
D. Manipulate format strings in text fields
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?
A. Use a scan tool like Nessus
B. Use the built-in Windows Update tool
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation
Answer: A (LEAVE A REPLY)
Explanation
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.
Note: Significant capabilities of Nessus include:
References:
http://searchnetworking.techtarget.com/definition/Nessus

NEW QUESTION: 136
Why should the security analyst disable/remove unnecessary ISAPI filters?
A. To defend against social engineering attacks
B. To defend against jailbreaking
C. To defend against webserver attacks
D. To defend against wireless attacks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
Which system consists of a publicly available set of databases that contain domain name registration contact information?
A. CAPTCHA
B. IETF
C. IANA
D. WHOIS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?
A. NMAP -P 192.168.0.0/16
B. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
C. NMAP -P 192.168.1-5.
D. NMAP -P 192.168.1/17
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?
A. Exclamation mark
B. Semicolon
C. Single quote
D. Double quote
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
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 field:

```
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. SQL injection

B. Cross-site request forgery

C. Command injection

D. Cross-site scripting

Answer: (SHOW ANSWER)

NEW QUESTION: 141

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL for FTP must be before the ACL 110

B. The ACL 104 needs to be first because is UDP

C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

D. The ACL 110 needs to be changed to port 80

Answer: (SHOW ANSWER)

NEW QUESTION: 142

An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is most likely able to handle this requirement?

A. RADIUS

B. DIAMETER

C. Kerberos

D. TACACS+

Answer: A (LEAVE A REPLY)

Explanation

Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks,

and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.
References: https://en.wikipedia.org/wiki/RADIUS

NEW QUESTION: 143
Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?
A. All of the employees would stop normal work activities
B. Not informing the employees that they are going to be monitored could be an invasion of privacy.
C. IT department would be telling employees who the boss is
D. The network could still experience traffic slow down.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
A. -P
B. -F
C. -r
D. -sP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
What is the difference between the AES and RSA algorithms?
A. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used
to encrypt data
B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used
to encrypt data
C. Both are asymmetric algorithms, but RSA uses 1024-bit keys
D. Both are symmetric algorithms, but AES uses 256-bit keys
Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.
What should you do?

A. Forward the message to your company's security response team and permanently delete the message from your computer.
B. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation
Answer: A (LEAVE A REPLY)
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.
References: https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_ConfigureScanEmailInboundAction.html

NEW QUESTION: 147
An attacker tries to do banner grabbing on a remote web server and executes the following command.

Service
detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
What did the hacker accomplish?
A. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.
B. The hacker successfully completed the banner grabbing.
C. The hacker should've used nmap -O host.domain.com.
D. nmap can't retrieve the version number of any running remote service.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.
What would Yancey be considered?

A. Since he does not care about going to jail, he would be considered a Black Hat
B. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing
C. Because Yancey works for the company currently; he would be a White Hat
D. Yancey would be considered a Suicide Hacker
Answer: D (LEAVE A REPLY)

NEW QUESTION: 149
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message.
The technique provides 'security through obscurity'.
What technique is Ricardo using?
A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption
Answer: A (LEAVE A REPLY)
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
References: https://en.wikipedia.org/wiki/Steganography

NEW QUESTION: 150
This asymmetry cipher is based on factoring the product of two large prime numbers.
What cipher is described above?
A. RSA
B. MD5
C. SHA
D. RC5
Answer: A (LEAVE A REPLY)

NEW QUESTION: 151
Company XYZ has asked you to assess the security of their perimeter email gateway.
From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.
Your email message looks like this:
From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com
Subject: Test message
Date: 4/3/2017 14:37
The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?

A. Email Masquerading
B. Email Spoofing
C. Email Harvesting
D. Email Phishing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
A security policy will be more accepted by employees if it is consistent and has the support of
A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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 device. This indicates that port 23 was not blocked at the firewall.
D. 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: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following is designed to identify malicious attempts to penetrate systems?
A. Intrusion Detection System

B. Firewall
C. Proxy
D. Router
Answer: A (LEAVE A REPLY)
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION: 155
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 router.
B. The host is likely a Windows machine.
C. The host is likely a printer.
D. The host is likely a Linux machine.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 156
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?
A. File system permissions

B. Privilege escalation
C. Directory traversal
D. Brute force login
Answer: A (LEAVE A REPLY)
Explanation
To upload files the user must have proper write file permissions.
References:
http://codex.wordpress.org/Hardening_WordPress

NEW QUESTION: 157
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?
A. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options
B. Performing common services for the application process and replacing real applications with fake ones
C. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
D. Defeating the scanner from detecting any code change at the kernel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 158
What would you enter, if you wanted to perform a stealth scan using Nmap?
A. nmap -sM
B. nmap -sU
C. nmap -sS
D. nmap -sT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 159
What is the main reason the use of a stored biometric is vulnerable to an attack?
A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
C. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.
D. A stored biometric is no longer "something you are" and instead becomes "something you have".
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
Look at the following output. What did the hacker accomplish?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168.1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```


A. The hacker successfully transferred the zone and enumerated the hosts.
B. The hacker used whois to gather publicly available records for the domain.
C. The hacker used the "fierce" tool to brute force the list of available domains.
D. The hacker listed DNS records on his own domain.
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Which statement is TRUE regarding network firewalls preventing Web Application attacks?
A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.
Answer: B (LEAVE A REPLY)
Explanation
Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.
References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

NEW QUESTION: 162

The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?
A. The document can be sent to the accountant using an exclusive USB for that document.
B. The CFO can use a hash algorithm in the document once he approved the financial statements.
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
D. The CFO can use an excel file with a password.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
The purpose of a _____is to deny network access to local area networks and other information assets
by unauthorized wireless devices.
A. Wireless Access Control List
B. Wireless Analyzer
C. Wireless Jammer
D. Wireless Access Point
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
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 (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 165
The "white box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 166
Which set of access control solutions implements two-factor authentication?
A. Fingerprint scanner and retina scanner
B. Account and password
C. USB token and PIN
D. Password and PIN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
An attacker with access to the inside network of a small company launches a successful STP manipulation
attack. What will he do next?
A. He will activate OSPF on the spoofed root bridge.
B. He will repeat the same attack against all L2 switches of the network.
C. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
D. He will repeat this action so that is escalates to a DoS attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
The company ABC recently contract a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What is the following options can be useful to ensure the integrity of the data?
A. The CFO can use a hash algorithm in the document once he approved the financial statements
B. The CFO can use an excel file with a password
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
D. The document can be sent to the accountant using an exclusive USB for that document

Answer: A (LEAVE A REPLY)

NEW QUESTION: 169
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 from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
C. Results for matches on target.com and Marketing,target.com that include the word "accounting"
D. Results matching "accounting" in domain target.com but not on the site Marketing.target.com
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?
A. The amount of time and resources that are necessary to maintain a biometric system.
B. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
C. How long it takes to setup individual user accounts.
D. The amount of time it takes to convert biometric data into a template on a smart card.
Answer: (SHOW ANSWER)

NEW QUESTION: 171
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.
Which of the following IP addresses could be teased as a result of the new configuration?
A. 10.1.4.254
B. 10.1.4.156
C. 10..1.5.200
D. 210.1.55.200
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.
Which Algorithm is this referring to?
A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access (WPA)
C. Wi-Fi Protected Access 2 (WPA2)

D. Temporal Key Integrity Protocol (TKIP)

Answer: (SHOW ANSWER)

Explanation

WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In

2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

NEW QUESTION: 173

You are monitoring the network of your organizations. You notice that:

1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication

Which of the following solution will you suggest?

A. Block the Blacklist IP's @ Firewall

B. Clean the Malware which are trying to Communicate with the External Blacklist IP's

C. Both B and C

D. Update the Latest Signatures on your IDS/IPS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 174

While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.Private.enter  [redacted].Cisco.[redacted].Cisco4700
system.sysUpTime.0 : Timeticks: (1563980[redacted] 18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which among the following can be used to get this output?

A. nmap protocol scan

B. An SNMP walk

C. A sniffer

D. A Bo2k system query.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 175

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer,""1111111111111111111111111111"");
}
```

Output:

Segmentation fault

A. Python

B. Java

C. C++

D. C#

Answer: C (LEAVE A REPLY)

NEW QUESTION: 176

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

A. Teardrop attack targeting 192.168.1.106

B. Port scan targeting 192.168.1.106

C. Denial of service attack targeting 192.168.1.103
D. Port scan targeting 192.168.1.103
Answer: B (LEAVE A REPLY)

NEW QUESTION: 177
What is the correct process for the TCP three-way handshake connection establishment and connection termination?
A. Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
C. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 178
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?
A. Burpsuite
B. Maskgen
C. Dimitry
D. Proxychains
Answer: A (LEAVE A REPLY)
Explanation
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
References: https://portswigger.net/burp/

NEW QUESTION: 179
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and
192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.
After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?
A. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Rootkit Attack
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 180
In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?
A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-plaintext attack
D. Adaptive chosen-plaintext attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?
A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan
Answer: (SHOW ANSWER)
Explanation
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run.
References: https://nmap.org/book/man-host-discovery.html

NEW QUESTION: 182
Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?
A. Protocol analyzer
B. Vulnerability scanner
C. Intrusion Detection System
D. Port scanner
Answer: (SHOW ANSWER)

NEW QUESTION: 183
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).
A. $62.5
B. $125
C. $65.2
D. $250
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following security policies defines the use of VPN for gaining access to an internal corporate
network?
A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy
Answer: (SHOW ANSWER)

NEW QUESTION: 185
While using your bank's online servicing you notice the following string in the URL bar:
"http: // www. MyPersonalBank. com/ account? id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount&Camount values and submit the request, that data on the web page reflects the changes.
Which type of vulnerability is present on this site?

A. XSS Reflection
B. SQL Injection
C. Cookie Tampering
D. Web Parameter Tampering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
In Wireshark, the packet bytes panes show the data of the current packet in which format?
A. Binary
B. Hexadecimal
C. Decimal
D. ASCII only
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?
A. PKI
B. single sign on
C. biometrics
D. SOA
Answer: (SHOW ANSWER)
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [1] and manage public- key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
References: https://en.wikipedia.org/wiki/Public_key_infrastructure

NEW QUESTION: 188
How do employers protect assets with security policies pertaining to employee surveillance activities?
A. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.
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 promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 189
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p -sl kiosk.adobe.com www.riaa.com kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-sl" with Nmap?
A. Conduct stealth scan
B. Conduct ICMP scan
C. Conduct IDLE scan
D. Conduct silent scan
Answer: (SHOW ANSWER)

NEW QUESTION: 190
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?
A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 191
Which of the below hashing functions are not recommended for use?
A. MD5, SHA-1
B. MD5. SHA-5
C. SHA-2. SHA-3
D. SHA-1.ECC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 192
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system.
Which TCP and UDP ports must you filter to check null sessions on your network?
A. 139 and 443
B. 137 and 443
C. 137 and 139
D. 139 and 445
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil
Corp's lobby. He checks his current SID, which is
S-1-5-21-1223352397-1872883824-861252104-501.
What needs to happen before Matthew has full administrator access?
A. He must perform privilege escalation.
B. He needs to disable antivirus protection.
C. He needs to gain physical access.
D. He already has admin privileges, as shown by the "501" at the end of the SID.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?
A. BeEF
B. Nessus
C. Metasploit
D. NMAP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
What is the role of test automation in security testing?
A. It is an option but it tends to be very expensive.
B. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace
manual testing completely.
C. It should be used exclusively. Manual testing is outdated because of low spend and possible test setup
inconsistencies.
D. Test automation is not usable in security due to the complexity of the tests.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196
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. 00001101 10100100
B. 00101000 11101110
C. 11010111 00010001

D. 11110010 01011011
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
Which of the following are well known password-cracking programs?
A. Jack the Ripper
B. Netbus
C. L0phtcrack
D. NetCat
E. John the Ripper
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. Snort
C. John the Ripper
D. Dsniff
Answer: A (LEAVE A REPLY)
Explanation
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over
1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

NEW QUESTION: 199

It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?
A. Threat
B. Attack
C. Vulnerability
D. Risk
Answer: A (LEAVE A REPLY)
Explanation
A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
References: https://en.wikipedia.org/wiki/Threat_(computer)

NEW QUESTION: 200
Some passwords are stored using specialized encryption algorithms known as hashes.
Why is this an appropriate method?
A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. Hashing is faster compared to more traditional encryption algorithms.
C. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 201
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. Email server certificate
B. Public key
C. Modulus length
D. Private key
Answer: (SHOW ANSWER)

NEW QUESTION: 202
A common cryptographical tool is the use of XOR. XOR the following binary values: 10110001 00111010
A. 11011000

B. 10001011
C. 10111100
D. 10011101
Answer: (SHOW ANSWER)

NEW QUESTION: 203
A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?
A. Avoid
B. Accept
C. Mitigate
D. Delegate
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users
without the recipient's consent, similar to email spamming?
A. Bluejacking
B. Bluesniffing
C. Bluesnarfing
D. Bluesmacking
Answer: A (LEAVE A REPLY)

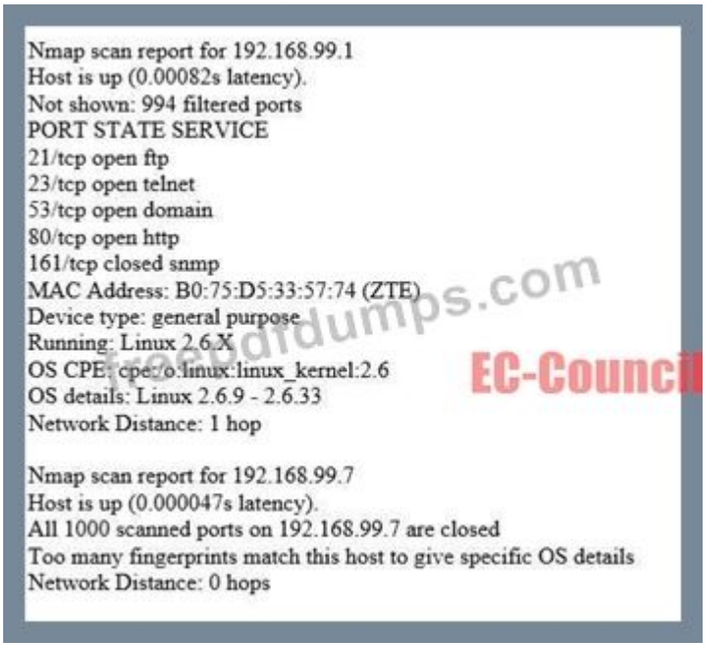
NEW QUESTION: 205
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?
A. She is using John the Ripper to view the contents of the file.
B. She is using John the Ripper to crack the passwords in the secret.txt file.
C. She is encrypting the file.
D. She is using ftp to transfer the file to another hacker named John.
Answer: (SHOW ANSWER)

NEW QUESTION: 206

Emil uses nmap to scan two hosts using this command:
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:



What is his conclusion?

A. Host 192.168.99.7 is an iPad.

B. Host 192.168.99.7 is down.

C. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7

D. Host 192.168.99.1 is the host that he launched the scan from.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 207

Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

A. Rootshell

B. Rootshock

C. Shellbash

D. Shellshock

Answer: D (LEAVE A REPLY)

NEW QUESTION: 208

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port
445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

A. Eve is trying to connect as a user with Administrator privileges
B. Eve is trying to carry out a password crack for user Administrator
C. Eve is trying to escalate privilege of the null user to that of Administrator
D. Eve is trying to enumerate all users with Administrative privileges
Answer: (SHOW ANSWER)

NEW QUESTION: 209
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What seems to be wrong?
A. OS Scan requires root privileges.
B. The nmap syntax is wrong.
C. This is a common behavior for a corrupted nmap application.
D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
Answer: (SHOW ANSWER)
Explanation
You requested a scan type which requires root privileges.
References:
http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

NEW QUESTION: 210
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. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
B. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.
C. Ask the employer for authorization to perform the work outside the company.
D. Start by foot printing the network and mapping out a plan of attack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
Which of the following is an extremely common IDS evasion technique in the web world?
A. unicode characters
B. spyware

C. port knocking
D. subnetting
Answer: A (LEAVE A REPLY)
Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.
One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.
References: http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html

NEW QUESTION: 212
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)
A. B757BF5C0D87772FAAD3B435B51404EE
B. 44EFCE164AB921CQAAD3B435B51404EE
C. BA810DBA98995F1817306D272A9441BB
D. 0182BD0BD4444BF836077A718CCDF409
E. E52CAC67419A9A224A3B108F3FA6CB6D
F. CEC52EB9C8E3455DC2265B23734E0DAC
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.
A. nmap -sn -sF 10.1.0.0/16 445
B. nmap -s 445 -sU -T5 10.1.0.0/16
C. nmap -p 445 -max -Pn 10.1.0.0/16
D. nmap -p 445 -n -T4 -open 10.1.0.0/16

Answer: D (LEAVE A REPLY)

NEW QUESTION: 214
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be
performed to determine their compliance with security policies. Which one of the following tools would most
likely be used in such an audit?
A. Intrusion Detection System
B. Vulnerability scanner
C. Port scanner
D. Protocol analyzer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 215
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?
A. >host -t a hackeddomain.com
B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com
Answer: A (LEAVE A REPLY)
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

NEW QUESTION: 216
Which of the following is optimized for confidential communications, such as bidirectional voice and video?
A. RC4
B. RC5
C. MD5
D. MD4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
D. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 218
You are doing an internal security audit and intend to find out what ports are open on all the servers. What is the best way to find out?
A. Scan servers with MBSA
B. Telnet to every port on each server
C. Scan servers with Nmap
D. Physically go to each server
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. tcpsplice
B. Burp
C. Whisker
D. Hydra
Answer: C (LEAVE A REPLY)

NEW QUESTION: 220
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```


How would you protect from these attacks?
A. Create rules in IDS to alert on strange Unicode requests

B. Configure the Web Server to deny requests involving "hex encoded" characters
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 221
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 extraneous queries.
B. Validate web content input for type, length, and range.
C. Validate web content input with scanning tools.
D. Validate web content input for query strings.
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Security and privacy of/on information systems are two entities that requires lawful regulations.
Which of the following regulations defines security and privacy controls for Federal information systems and organizations?
A. PCI-DSS
B. HIPAA
C. EU Safe Harbor
D. NIST SP 800-53
Answer: D (LEAVE A REPLY)

NEW QUESTION: 223
Which of these options is the most secure procedure for storing backup tapes?
A. Inside the data center for faster retrieval in a fireproof safe
B. On a different floor in the same building
C. In a cool dry environment
D. In a climate controlled facility offsite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 224
What is the code written for?

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMO
N.","GDOG.","KSTET.","GTER.","HTER.","LTER.","KSTAN."]
for command in commands:
 for buffstring in buffer:
  print "Exploiting" +command+":"+str(len(buffstring))
  s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
  s.connect(('127.0.0.1',9999))
  s.recv(50)
  s.send(command+buffstring)
  s.close()
```


A. Encryption
B. Buffer Overflow
C. Denial-of-service (Dos)
D. Bruteforce
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?
A. ARP is disabled on the target server
B. You need to run the ping command with root privileges
C. ICMP could be disabled on the target server
D. TCP/IP doesn't support ICMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 226
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability
C. SQL injection vulnerability

D. Web site defacement vulnerability

Answer: A (LEAVE A REPLY)

Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION: 227

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 (LEAVE A REPLY)

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

References: https://en.wikipedia.org/wiki/Macro_virus

NEW QUESTION: 228

While performing online banking using a Web browser, a user receives an email that contains a link to an

interesting Web site. When the user clicks on the link, another Web browser session starts and displays a

video of cats playing a piano. The next business day, the user receives what looks like an email from his
bank, indicating that his bank account has been accessed from a foreign country. The email asks the user
to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based
security vulnerability was exploited to compromise the user?
A. Cross-Site Scripting
B. Cross-Site Request Forgery
C. Clickjacking
D. Web form input validation
Answer: (SHOW ANSWER)

NEW QUESTION: 229
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer.
What is the consultant's obligation to the financial organization?
A. Stop work immediately and contact the authorities.
B. Delete the pornography, say nothing, and continue security testing.
C. Bring the discovery to the financial organization's human resource department.
D. Say nothing and continue with the security testing.
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?
A. NET USE
B. NET CONFIG
C. NET FILE
D. NET VIEW
Answer: A (LEAVE A REPLY)
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.
References: https://technet.microsoft.com/en-us/library/bb490717.aspx

NEW QUESTION: 231
Bob learned that his username and password for a popular game has been compromised. He contacts the

company and resets all the information. The company suggests he use two-factor authentication; which
option below offers that?
A. Disable his username and use just a fingerprint scanner
B. A fingerprint scanner and his username and password
C. His username and a stronger password
D. A new username and password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?
A. Vulnerability assessment
B. Active information gathering
C. Information reporting
D. Passive information gathering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 233
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?
A. Hire a security consultant to provide direction.
B. Back up the hashes of the credit card numbers not the actual credit card numbers.
C. Do not back up either the credit card numbers or their hashes.
D. Encrypt backup tapes that are sent off-site.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
A. Armitage
B. Nikto
C. Metasploit
D. Nmap
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 235
Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)
A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
C. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111
D. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
Answer: C (LEAVE A REPLY)

NEW QUESTION: 236
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?
A. File system permissions
B. Privilege escalation
C. Directory traversal
D. Brute force login
Answer: (SHOW ANSWER)
To upload files the user must have proper write file permissions.
References: http://codex.wordpress.org/Hardening_WordPress

NEW QUESTION: 237
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?
A. 110
B. 135
C. 445
D. 161
E. 139
F. 1024
Answer: (SHOW ANSWER)

NEW QUESTION: 238
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?
A. The company accepting bids will want the same type of format of testing.
B. The company accepting bids will hire the consultant because of the great work performed.
C. The consultant will ask for money on the bid because of great work.
D. The consultant may expose vulnerabilities of other companies.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 239
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?
A. Windowing
B. Hardening
C. Harvesting
D. Stealthing
Answer: (SHOW ANSWER)

NEW QUESTION: 240
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?
A. openssl_client -site www.website.com:443
B. openssl_client -connect www.website.com:443
C. openssl s_client -site www.website.com:443
D. openssl s_client -connect www.website.com:443
Answer: D (LEAVE A REPLY)