



## **EC-Council**

### **Exam Questions 312-50v13**

Certified Ethical Hacker v13

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Topic 1)

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.

Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

- A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

**Answer:** A

### NEW QUESTION 2

- (Topic 1)

What two conditions must a digital signature meet?

- A. Has to be the same number of characters as a physical signature and must be unique.
- B. Has to be unforgeable, and has to be authentic.
- C. Must be unique and have special characters.
- D. Has to be legible and neat.

**Answer:** B

### NEW QUESTION 3

- (Topic 1)

??.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of

unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.??

Fill in the blank with appropriate choice.

- A. Evil Twin Attack
- B. Sinkhole Attack
- C. Collision Attack
- D. Signal Jamming Attack

**Answer:** A

#### **Explanation:**

[https://en.wikipedia.org/wiki/Evil\\_twin\\_\(wireless\\_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that

looks like a legitimate access point to steal victims?? sensitive details. Most often, the victims of such attacks are ordinary people like you and me.

The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.

An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.

ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

### NEW QUESTION 4

- (Topic 1)

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- A. Honeypots
- B. Firewalls
- C. Network-based intrusion detection system (NIDS)
- D. Host-based intrusion detection system (HIDS)

**Answer:** C

### NEW QUESTION 5

- (Topic 1)

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

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

Answer: B

#### NEW QUESTION 6

- (Topic 1)

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

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

Answer: A

#### NEW QUESTION 7

- (Topic 1)

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. Resource records
- C. Resource transfer
- D. Zone transfer

Answer: A

#### Explanation:

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by DNS for use on IP networks. DNSSEC is a set of extensions to DNS provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. DNSSEC is necessary because the original DNS design did not include security but was designed to be a scalable distributed system. DNSSEC adds security while maintaining backward compatibility.

#### NEW QUESTION 8

- (Topic 1)

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

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

Answer: D

#### Explanation:

«Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.»

Did you know that the EC-Council exam shows how well you know their official book? So, there is no "Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.

[https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system\\_evasion\\_techniques](https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques)

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'.

By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.

NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

#### NEW QUESTION 9

- (Topic 1)

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permiscuous
- D. AH Tunnel mode

Answer: A

#### NEW QUESTION 10

- (Topic 1)

Which of the following is not a Bluetooth attack?

- A. Bluedriving

- B. Bluesmacking
- C. Bluejacking
- D. Bluesnarfing

**Answer:** A

**Explanation:**

<https://github.com/verovaleros/bluedriving>

Bluedriving is a bluetooth wardriving utility. It can capture bluetooth devices, lookup their services, get GPS information and present everything in a nice web page. It can search for and show a lot of information about the device, the GPS address and the historic location of devices on a map. The main motivation of this tool is to research about the targeted surveillance of people by means of its cellular phone or car. With this tool you can capture information about bluetooth devices and show, on a map, the points where you have seen the same device in the past.

**NEW QUESTION 10**

- (Topic 1)

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

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

**Answer:** C

**NEW QUESTION 14**

- (Topic 1)

What kind of detection techniques is being used in antivirus software 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. Behavioral based
- B. Heuristics based
- C. Honeypot based
- D. Cloud based

**Answer:** D

**NEW QUESTION 15**

- (Topic 1)

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

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

**Answer:** E

**NEW QUESTION 18**

- (Topic 1)

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right
- C. He does not need to separate networks if he can create rules by destination IPs, one by one
- D. Bob is totally wrong
- E. DMZ is always relevant when the company has internet servers and workstations
- F. Bob is partially right
- G. DMZ does not make sense when a stateless firewall is available

**Answer:** C

**NEW QUESTION 21**

- (Topic 1)

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Randomizing
- B. Bounding
- C. Mutating
- D. Fuzzing

Answer: D

#### NEW QUESTION 24

- (Topic 1)

You are the Network Admin, and you get a complaint 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 53
- B. Traffic is Blocked on TCP Port 80
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

Answer: A

#### Explanation:

Most likely have an issue with DNS.

DNS stands for Domain Name System. It's a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server's unique ID where a website is stored.

Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.

NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.

The 8 steps in a DNS lookup:

- \* 1. A user types example.com into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
- \* 2. The resolver then queries a DNS root nameserver;
- \* 3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
- \* 4. The resolver then requests the .com TLD;
- \* 5. The TLD server then responds with the IP address of the domain's nameserver, example.com;
- \* 6. Lastly, the recursive resolver sends a query to the domain's nameserver;
- \* 7. The IP address for example.com is then returned to the resolver from the nameserver;
- \* 8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially;

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:

- \* 9. The browser makes an HTTP request to the IP address;
- \* 10. The server at that IP returns the webpage to be rendered in the browser.

NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

#### NEW QUESTION 27

- (Topic 1)

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- A. tcptrace
- B. Nessus
- C. OpenVAS
- D. tcptraceroute

Answer: A

#### NEW QUESTION 28

- (Topic 1)

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

- A. Birthday
- B. Brute force
- C. Man-in-the-middle
- D. Smurf

Answer: B

#### NEW QUESTION 33

- (Topic 1)

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Boot.ini
- B. Sudoers
- C. Networks
- D. Hosts

Answer: D

#### NEW QUESTION 36

- (Topic 1)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

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

**Answer:** ABD

#### NEW QUESTION 38

- (Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 42

- (Topic 1)

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

A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

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

**Answer:** B

#### NEW QUESTION 46

- (Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 50

- (Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 54

- (Topic 1)

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

- A. Man-in-the-middle attack
- B. Meet-in-the-middle attack
- C. Replay attack
- D. Traffic analysis attack

**Answer:** B

#### Explanation:

[https://en.wikipedia.org/wiki/Meet-in-the-middle\\_attack](https://en.wikipedia.org/wiki/Meet-in-the-middle_attack)

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space–time tradeoff cryptographic attack against encryption schemes that rely on

performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations.

The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

#### NEW QUESTION 59

- (Topic 1)

Which of the following tools are used for enumeration? (Choose three.)

- A. SolarWinds
- B. USER2SID
- C. Cheops
- D. SID2USER
- E. DumpSec

**Answer:** BDE

#### NEW QUESTION 61

- (Topic 1)

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. Piggybacking
- C. Tailgating
- D. Eavesdropping

**Answer:** A

#### Explanation:

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

#### NEW QUESTION 62

- (Topic 1)

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- A. John the Ripper
- B. SET
- C. CHNTPW
- D. Cain & Abel

**Answer:** C

#### NEW QUESTION 64

- (Topic 1)

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

**Answer:** BCDE

#### NEW QUESTION 66

- (Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 68

- (Topic 1)

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

- A. Linux
- B. Unix
- C. OS X
- D. Windows

**Answer: D**

#### NEW QUESTION 72

- (Topic 1)

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

**Answer: A**

#### NEW QUESTION 75

- (Topic 1)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

**Answer: A**

#### Explanation:

[https://en.wikipedia.org/wiki/Kismet\\_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

#### NEW QUESTION 79

- (Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 81

- (Topic 1)

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

**Answer: C**

#### NEW QUESTION 85

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

[https://en.wikipedia.org/wiki/Private\\_network](https://en.wikipedia.org/wiki/Private_network)

In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments.

Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet.

However, several technologies allow such machines to connect to the Internet.

- Mediation servers like IRC, Usenet, SMTP and Proxy server
- Network address translation (NAT)
- Tunneling protocol

NOTE: So, the problem is just one of these technologies.

#### NEW QUESTION 88

- (Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 92

- (Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 93

- (Topic 1)

Which of the following is assured by the use of a hash?

- A. Authentication
- B. Confidentiality
- C. Availability
- D. Integrity

**Answer: D**

#### NEW QUESTION 98

- (Topic 1)

Which of the following program infects the system boot sector and the executable files at the same time?

- A. Polymorphic virus
- B. Stealth virus
- C. Multipartite Virus
- D. Macro virus

**Answer: C**

#### NEW QUESTION 99

- (Topic 1)

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?

```

45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..î(.ø.2...Ñ:.....
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO@.}pxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvY..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿç !÷ÿç"÷ÿç#÷ÿçXX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1à°FÍ..Å10°f.Đ
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mù.MóÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ifÇEi.'.Mô
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Ei.EøEEù..Đ.MóÍ..ĐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ĐCÍ..Å1É*?.ĐÍ..Đ
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.è.^ .u.1à.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èäÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)

```

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

Answer: D

**NEW QUESTION 104**

- (Topic 1)  
 Which results will be returned with the following Google search query? site:target.com – site:Marketing.target.com accounting

- A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
- B. Results matching all words in the query.
- 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: D

**NEW QUESTION 107**

- (Topic 1)  
 Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering
- B. Eavesdropping
- C. Scanning
- D. Sniffing

Answer: A

**NEW QUESTION 109**

- (Topic 1)  
 Study the following log extract and identify the attack.

```

12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 2D 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./...../...../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 2D 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, =/?..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-EncodD
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 2D 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....

```

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

Answer: D

**NEW QUESTION 110**

-(Topic 1)

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. Cookie Tampering
- B. SQL Injection
- C. Web Parameter Tampering
- D. XSS Reflection

Answer: C

**NEW QUESTION 112**

-(Topic 1)

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 -r 10.10.1.0/24
- D. nmap -T4 -O 10.10.0.0/24

**Answer: B**

**Explanation:**

<https://nmap.org/book/man-port-specification.html>

NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.

«nmap -T4 -F 10.10.0.0/24» This option is "correct" because of the -F flag.

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100. Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

**NEW QUESTION 114**

- (Topic 1)

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**

**NEW QUESTION 119**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Modernization Act of 2014 (FISMA) and to help with managing cost-effective programs to protect their information and information systems.

**NEW QUESTION 123**

- (Topic 1)

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

**Answer: A**

**NEW QUESTION 126**

- (Topic 1)

Which of the following describes the characteristics of a Boot Sector Virus?

- A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
- B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
- C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
- D. Overwrites the original MBR and only executes the new virus code.

**Answer: C**

**NEW QUESTION 130**

- (Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

**Answer:** B

#### NEW QUESTION 132

- (Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 135

- (Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 138

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not

False Negative - IDS referring a behavior not an attack, but in real life is an attack. False Negative - is the most serious and dangerous state of all !!!!

#### NEW QUESTION 139

- (Topic 1)

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

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

**Answer:** BCE

#### NEW QUESTION 143

- (Topic 1)

One of your team members has asked you to analyze the following SOA record. What is the version?  
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

**Answer:** A

#### NEW QUESTION 147

- (Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 148

- (Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 151

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

<https://www.wireshark.org/>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

#### NEW QUESTION 154

- (Topic 1)

What did the following commands determine?

```
C: user2sid \earth guest
s-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

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

**Answer: D**

#### NEW QUESTION 158

- (Topic 1)

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A. Spanning tree
- B. Dynamic ARP Inspection (DAI)
- C. Port security
- D. Layer 2 Attack Prevention Protocol (LAPP)

**Answer: B**

**Explanation:**

Dynamic ARP inspection (DAI) protects switching devices against Address Resolution Protocol (ARP) packet spoofing (also known as ARP poisoning or ARP cache poisoning). DAI inspects ARPs on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

**NEW QUESTION 163**

- (Topic 1)

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

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

**Answer: D**

**NEW QUESTION 166**

- (Topic 1)

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

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

**Answer: B**

**NEW QUESTION 170**

- (Topic 1)

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

**Answer: A**

**NEW QUESTION 174**

- (Topic 1)

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

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

**Answer: D**

**NEW QUESTION 176**

- (Topic 1)

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

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

**Answer: A**

**NEW QUESTION 180**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

[https://en.wikipedia.org/wiki/Sniffing\\_attack](https://en.wikipedia.org/wiki/Sniffing_attack)

To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.

NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors.

The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

**NEW QUESTION 182**

- (Topic 1)

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

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

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

**Answer: D**

**NEW QUESTION 186**

- (Topic 1)

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end- to-end encryption of the connection?

- A. SFTP
- B. Ipsec
- C. SSL
- D. FTPS

**Answer: B**

**Explanation:**

<https://en.wikipedia.org/wiki/IPsec>

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs). IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

**NEW QUESTION 187**

- (Topic 1)

CompanyXYZ 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 CompanyXYZ. The employee of CompanyXYZ 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 CompanyXYZ receives your email message.

This proves that CompanyXYZ??s email gateway doesn??t prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

**Answer: D**

**Explanation:**

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is common for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems and sometimes pose a real security threat.

**NEW QUESTION 190**

- (Topic 1)

What is the role of test automation in security testing?

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

F. But it cannot replace manual testing completely.

**Answer:** D

#### NEW QUESTION 192

- (Topic 1)

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- B. Network sniffer
- C. Intrusion Prevention System (IPS)
- D. Vulnerability scanner

**Answer:** A

#### NEW QUESTION 195

- (Topic 1)

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 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 a 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

#### Explanation:

File system permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

#### NEW QUESTION 198

- (Topic 1)

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 create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.

**Answer:** A

#### NEW QUESTION 200

- (Topic 1)

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

However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

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

**Answer:** B

#### NEW QUESTION 201

- (Topic 1)

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

**Answer:** B

#### NEW QUESTION 202

- (Topic 1)

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

What is this type of DNS configuration commonly called?

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

**Answer: D**

#### NEW QUESTION 203

- (Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 207

- (Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 208

- (Topic 2)

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack' or 1=1 - Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

- A. select \* from Users where UserName = 'attack" or 1=1 -- and UserPassword = '123456'
- B. select \* from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
- C. select \* from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
- D. select \* from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

**Answer: D**

#### NEW QUESTION 211

- (Topic 2)

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

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

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

**Answer: C**

#### NEW QUESTION 213

- (Topic 2)

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- A. Union-based SQLi
- B. Out-of-band SQLi
- C. In-band SQLi
- D. Time-based blind SQLi

**Answer: B**

**Explanation:**

Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp\_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL\_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

**NEW QUESTION 216**

- (Topic 2)

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. Which two SQL Injection types would give her the results she is looking for?

- A. Out of band and boolean-based
- B. Time-based and union-based
- C. Union-based and error-based
- D. Time-based and boolean-based

**Answer: D**

**Explanation:**

Boolean based we mean that it is based on Boolean values, that is, true or false / true and false. AND Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

<https://www.acunetix.com/websitesecurity/sql-injection2/>

**NEW QUESTION 221**

- (Topic 2)

The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

- A. Regularly test security systems and processes.
- B. Encrypt transmission of cardholder data across open, public networks.
- C. Assign a unique ID to each person with computer access.
- D. Use and regularly update anti-virus software on all systems commonly affected by malware.

**Answer: C**

**NEW QUESTION 223**

- (Topic 2)

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 802.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

- A. MQTT
- B. LPWAN
- C. Zigbee
- D. NB-IoT

**Answer: C**

**Explanation:**

Zigbee could be a wireless technology developed as an open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of 4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003.

The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee 3.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance. Over three hundred leading semiconductor makers, technology

corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

#### THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

- ? Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- ? Low duty cycle – provides long battery life
- ? Low latency
- ? Direct Sequence unfold Spectrum (DSSS)
- ? Up to 65,000 nodes per network
- ? 128-bit AES encryption for secure information connections
- ? Collision avoidance, retries and acknowledgements

This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

#### NEW QUESTION 228

- (Topic 2)

Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ??' or '1='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

- A. Null byte
- B. IP fragmentation
- C. Char encoding
- D. Variation

**Answer: D**

#### Explanation:

One may append the comment ??–?? operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead.

To launch such an attack, the value passed for name could be ??OR ??1??=??1?? ; —Statement = ??SELECT \* FROM ??CustomerDB?? WHERE ??name?? = ?? ??+ userName + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ??

Statement = ??SELECT \* FROM ??CustomerDB?? WHERE ??name?? = ?? ?? OR ??1??=??1??;- + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ?? All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn??t strongly used in or isn??t checked for sort constraints.

This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as ??' or '1='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments.

Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as ??' or '1='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as ??true?? so that any mathematical or string comparison can be used, where the SQL can perform the same.

#### NEW QUESTION 231

- (Topic 2)

which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

- A. Bluesmacking
- B. Bluebugging
- C. Bluejacking
- D. Bluesnarfing

**Answer: D**

#### Explanation:

Bluesnarfing is the unauthorized access of information from a wireless device through aBluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

#### NEW QUESTION 236

- (Topic 2)

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. Netcraft
- C. infoga
- D. Zoominfo

**Answer: C**

**Explanation:**

Infoga may be a tool gathering email accounts informations (ip,hostname,country,??) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

**NEW QUESTION 241**

- (Topic 2)

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

- A. verification
- B. Risk assessment
- C. Vulnerability scan
- D. Remediation

**Answer: D**

**Explanation:**

Vulnerability-Management Life Cycle The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. 4.Remediation - applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. (P.515/499)

**NEW QUESTION 243**

- (Topic 2)

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

**Answer: BE**

**NEW QUESTION 247**

- (Topic 2)

jane, an ethical hacker. Is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

- A. website mirroring
- B. Session hijacking
- C. Web cache poisoning
- D. Website defacement

**Answer: A**

**Explanation:**

A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites.A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience.If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded.Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access.Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.

**NEW QUESTION 248**

- (Topic 2)

Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

- A. Medium
- B. Low
- C. Critical
- D. High

**Answer: A**

**Explanation:**

Rating CVSS Score None 0.0  
Low 0.1 - 3.9  
Medium 4.0 - 6.9  
High 7.0 - 8.9

Critical 9.0 - 10.0

<https://www.first.org/cvss/v3.0/specification-document>

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Qualitative Severity Rating Scale

For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

**NEW QUESTION 250**

- (Topic 2)

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

- A. Preparation
- B. Eradication
- C. Incident recording and assignment
- D. Incident triage

**Answer: D**

**Explanation:**

Incident Handling and Response Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. Steps involved in the IH&R process: 3.Incident Triage - The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited. (P.84/68)

**NEW QUESTION 253**

- (Topic 2)

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

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

**Answer: C**

**NEW QUESTION 257**

- (Topic 2)

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

- A. The attacker queries a nameserver using the DNS resolver.
- B. The attacker makes a request to the DNS resolver.
- C. The attacker forges a reply from the DNS resolver.
- D. The attacker uses TCP to poison the DNS resolver.

**Answer: B**

**Explanation:**

[https://ru.wikipedia.org/wiki/DNS\\_spoofing](https://ru.wikipedia.org/wiki/DNS_spoofing)  
 DNS spoofing is a threat that copies the legitimate server destinations to divert the

domain's traffic. Ignoring these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

#### NEW QUESTION 262

- (Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 265

- (Topic 2)

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

- A. use of command-line interface
- B. Data staging
- C. Unspecified proxy activities
- D. Use of DNS tunneling

**Answer: C**

#### Explanation:

A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy. If you're employing a proxy server, internet traffic flows through the proxy server on its behalf to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. Once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

#### NEW QUESTION 266

- (Topic 2)

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

**Answer: D**

#### NEW QUESTION 268

- (Topic 2)

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Quid pro quo
- B. Diversion theft
- C. Elicitation
- D. Phishing

**Answer: A**

#### Explanation:

<https://www.eccouncil.org/what-is-social-engineering/>

This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician. The con artist asks for the login credentials of the company's computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company's computer and may possibly load malware or steal personal information that can be a motive to commit identity theft.

"A quid pro quo attack (aka something for something?? attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action." <https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.>

#### NEW QUESTION 273

- (Topic 2)

To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

- A. Hypervisor rootkit
- B. Kernel toolkit
- C. Hardware rootkit
- D. Firmware rootkit

**Answer: B**

#### Explanation:

Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel-mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

#### NEW QUESTION 277

- (Topic 2)

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven??s iPhone through the infected computer and is able to monitor and read all of Steven??s activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

- A. IOS trustjacking
- B. IOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

**Answer: A**

#### Explanation:

An iPhone client??s most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called ??Trustjacking??, which permits an aggressor to do precisely that. This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the ??iTunes Wi-Fi sync?? highlight, which makes it conceivable to proceed with this sort of correspondence

with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering ??iTunes Wi-Fi sync?? doesn??t need the casualty??s endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget??s screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn??t anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

#### NEW QUESTION 278

- (Topic 2)

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-4: Orchestrators
- C. Tier-3: Registries
- D. Tier-2: Testing and accreditation systems

**Answer: D**

#### Explanation:

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical,

managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to

refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

#### NEW QUESTION 280

- (Topic 2)

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

- A. Phishing malware
- B. Zero-day malware
- C. File-less malware
- D. Logic bomb malware

**Answer: C**

#### Explanation:

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html>

Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. Also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. It resides in the system's RAM. It injects malicious code into the running processes. (P.966/950)

#### NEW QUESTION 284

- (Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 287

- (Topic 2)

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

How would an attacker exploit this design by launching TCP SYN attack?

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

**Answer: B**

#### NEW QUESTION 291

- (Topic 2)

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

- A. Credentialed assessment
- B. Database assessment
- C. Host-based assessment
- D. Distributed assessment

**Answer: C**

#### Explanation:

The host-based vulnerability assessment (VA) resolution arose from the auditors' need to periodically review systems. Arising before the net becoming common, these tools typically take an administrator's eye read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. Uses Host VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. It should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans are unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

#### What it Measures Host

VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally ??dormant?? vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

#### NEW QUESTION 296

- (Topic 2)

What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

- A. Vulnerability hunting program
- B. Bug bounty program
- C. White-hat hacking program
- D. Ethical hacking program

**Answer: B**

#### Explanation:

Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.

The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and

run) a program curated to the organization??s wants.

Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).

Who uses bug bounty programs?Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you??ll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.

Why do corporations use bug bounty programs?Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code. This gives them access to a bigger variety of hackers or testers than they??d be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.

It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.

This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.

Why do researchers and hackers participate in bug bounty programs?Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.

It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.

What area unit the disadvantages of a bug bounty program for independent researchers and hackers?A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.

In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.

Roughly ninety seven of participants on major bug bounty platforms haven??t sold-out a bug. In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform. Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).

What square measure the disadvantages of bug bounty programs for organizations?These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren??t able to find themselves (and if they??ll fix those problems)! If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.

Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it??s probably that they??re going to receive quite few unhelpful reports for each useful report).

Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.

The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.

This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.

This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations?? product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

#### NEW QUESTION 301

- (Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 306

- (Topic 2)

Henry is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the UnKornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

- A. 64
- B. 128
- C. 255
- D. 138

**Answer: B**

#### Explanation:

Windows TTL 128, Linux TTL 64, OpenBSD 255 ... <https://subinsb.com/default-device-ttl-values/>

Time to Live (TTL) represents the number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

#### NEW QUESTION 307

- (Topic 2)

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

- A. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

**Answer: A**

#### NEW QUESTION 310

- (Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 311

- (Topic 2)

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. HIPAA/PHI
- B. PII
- C. PCIDSS
- D. ISO 2002

**Answer: A**

#### Explanation:

PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. Under HIPAA PHI is considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a aid clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.

It is not only past and current medical info that's considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health info in any kind, together with physical records, electronic records, or spoken info. Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of PHI underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info.

The eighteen identifiers that create health info letter are:

- ? Names
- ? Dates, except year
- ? phone numbers
- ? Geographic information
- ? FAX numbers
- ? Social Security numbers
- ? Email addresses
- ? case history numbers
- ? Account numbers
- ? Health arrange beneficiary numbers
- ? Certificate/license numbers
- ? Vehicle identifiers and serial numbers together with license plates
- ? Web URLs
- ? Device identifiers and serial numbers

- ? net protocol addresses
- ? Full face photos and comparable pictures
- ? Biometric identifiers (i.e. retinal scan, fingerprints)
- ? Any distinctive identifying variety or code

One or a lot of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

### NEW QUESTION 313

- (Topic 2)

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

- A. Pretexting
- B. Pharming
- C. Wardriving
- D. Skimming

**Answer: B**

#### Explanation:

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data. Though they share similar goals, pharming uses a special technique from phishing. Pharming attacker are targeted on manipulating a system, instead of tricking people into

reaching to a dangerous web site, explains David Emm, principal security man of science at Kaspersky. When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different.

### NEW QUESTION 318

- (Topic 2)

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

- A. JSON-RPC
- B. SOAP API
- C. RESTful API
- D. REST API

**Answer: C**

#### Explanation:

\*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. \*RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as RESTful APIs:

- o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing
- o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

<https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf>

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

### NEW QUESTION 320

- (Topic 2)

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

- A. WEP
- B. RADIUS
- C. WPA
- D. WPA3

**Answer: A**

#### Explanation:

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy. A research group from the University of California at Berkeley recently published a report citing major security flaws in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks.

The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP– which is included in many networking products – was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it??s very effective.

#### NEW QUESTION 322

- (Topic 2)

joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

- A. Cloud booker
- B. Cloud consumer
- C. Cloud carrier
- D. Cloud auditor

**Answer: C**

#### Explanation:

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc. The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

#### NEW QUESTION 324

- (Topic 2)

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

- A. openssl s\_client -site www.website.com:443
- B. openssl\_client -site www.website.com:443
- C. openssl s\_client -connect www.website.com:443
- D. openssl\_client -connect www.website.com:443

**Answer: C**

#### NEW QUESTION 325

- (Topic 2)

How does a denial-of-service attack work?

- A. A hacker prevents a legitimate user (or group of users) from accessing a service
- B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
- C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
- D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

**Answer: A**

#### NEW QUESTION 328

- (Topic 2)

Which utility will tell you in real time which ports are listening or in another state?

- A. Netstat
- B. TCPView
- C. Nmap
- D. Loki

**Answer: B**

#### NEW QUESTION 330

- (Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 332

- (Topic 2)

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES

- C. SHA
- D. SSL

**Answer:** B

### NEW QUESTION 333

- (Topic 2)

Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Distributed assessment
- B. Wireless network assessment
- C. Host-based assessment
- D. Application assessment

**Answer:** B

#### Explanation:

Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network. Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system. Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner. This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment. It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses. Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

### NEW QUESTION 337

- (Topic 2)

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

- A. ophcrack
- B. Hootsuite
- C. VisualRoute
- D. HULK

**Answer:** B

#### Explanation:

Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role. With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI. There area unit many totally different plans to decide on from, from one user set up up to a bespoke enterprise account that's appropriate for much larger organizations. Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

### NEW QUESTION 338

- (Topic 2)

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Phishing
- B. Vishing
- C. Spoofing
- D. DDoS

**Answer:** A

#### Explanation:

<https://en.wikipedia.org/wiki/Phishing>  
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

#### NEW QUESTION 340

- (Topic 2)

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN
- B. RST
- C. PSH
- D. URG
- E. FIN

**Answer: C**

#### NEW QUESTION 341

- (Topic 2)

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

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

**Answer: BD**

#### NEW QUESTION 343

- (Topic 2)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

- A. Nmap
- B. Cain & Abel
- C. Nessus
- D. Snort

**Answer: D**

#### NEW QUESTION 346

- (Topic 2)

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

- A. Use his own public key to encrypt the message.
- B. Use Marie's public key to encrypt the message.
- C. Use his own private key to encrypt the message.
- D. Use Marie's private key to encrypt the message.

**Answer: B**

#### Explanation:

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key

[https://en.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](https://en.wikipedia.org/wiki/Pretty_Good_Privacy)

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

[https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with

anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

#### NEW QUESTION 349

- (Topic 2)

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80

**Answer: C**

#### Explanation:

TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the most protocols in TCP/IP networks. transmission control protocol could be a connection-oriented protocol, it needs acknowledgement to line up end- to-end communications. only a association is about up user??s knowledge may be sent bi- directionally over the association.

Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn't have bonded communication as transmission control protocol.

UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.

UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).

Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. several internet applications use UDP, e.g. the name System (DNS), the Routing info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

#### NEW QUESTION 350

- (Topic 2)

While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed. What most likely happened?

- A. Matt inadvertently provided the answers to his security questions when responding to the post.
- B. Matt's bank-account login information was brute forced.
- C. Matt Inadvertently provided his password when responding to the post.
- D. Matt's computer was infected with a keylogger.

**Answer: A**

#### NEW QUESTION 354

.....

## Relate Links

**100% Pass Your 312-50v13 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/312-50v13-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>