Question # 1

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Answer: A

Question # 2

A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help accomplish this goal?

A. Classify the data

B. Mask the data

C. Assign an application owner

D. Perform a risk analysis

Answer: A

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently.

Question #:3

A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

A. laaS

B. PasS

C. MaaS

D. SaaS

Answer: D

It is not stating what type of devices, just BYOD, so cannot tell which platform is needed, or what requirements are involved

MAAS (*Metal as a Service*)

Question #:4

An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk

A. avoidance

B. acceptance

C. mitigation

D. transference

Answer: D

Risk Transference is transferring risk to a third party such as a vendor. In cyber security, that can be through utilizing cyber-risk insurance. Cyber insurance generally covers a business' liability for a data breach involving sensitive customer information, such as account numbers, credit card numbers, health records etc.

Question #:5

The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs. Which of the following is the BEST solution to meet the requirement?

A. Tokenization

B. Masking

C. Full disk encryption

D. Mirroring

Answer: A

Tokenization is mainly used to protect data at rest whereas masking is used to protect data in use

1. You can reverse tokenization

2. You can tokenize specific fields

3. You cannot reverse masking (You lose the credit card data)

4. Whenever you see credit card data, social security numbers etc that need to be protected always choose tokenization

5. If you see that you need to have real data in a testing server to test functionality but don't want to leak PII then use masking to substitute that data!

Question #:6

A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

A. SaaS

B. IaaS

C. PaaS

D. SDN

Answer: A

Explanation

In order from the least amount of management, to the most amount of management for the company:

SaaS > PaaS > IaaS > On-site

SaaS - Basically everything is managed by the provider

PaaS - The provider manages everything other than applications and data

IaaS - The middle-ground of services. The provider takes on half, while you take on the other half. Provider is responsible for virtualization, networking, servers, and storage. The company is responsible for applications, data, runtime, OS, and middleware.

On-site - There is no service provider. The company is responsible for the whole pie.

https://www.pcmag.com/picks/the-best-database-as-a-service-solutions

Question #:7

A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

A. Autopsy

B. Memdump

C. FTK imager

D. Wireshark

Answer: D

Explanation

Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

Question #:8

A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021 - 18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021 - 18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021 - 18:00:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021 - 18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021 - 18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

Which of the following explains these log entries?

A. SQL injection and improper input-handling attempts

B. Cross-site scripting and resource exhaustion attempts

C. Command injection and directory traversal attempts

D. Error handling and privilege escalation attempts

Answer: C

Directory traversal is when an attacker uses the software on a web server to access data in a directory other than the server's root directory. If the attempt is successful, the threat actor can view restricted files or execute commands on the server.

Command injection is an attack that involves executing commands on a host. Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation.

The attacker is attempting to traverse the directory of the host and execute the cat command which could be used to print the contents of a file.

Question #:9

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Answer: B

A USB data blocker, is a device that allows you to plug into USB charging ports including charging kiosks, and USB ports on gadgets owned by other people.

The main purpose of using one is to eliminate the risk of infecting your phone or tablet with malware, and even prevent hackers to install/execute any malicious code to access your data.

Question #:10

A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools, if available on the server, will provide the MOST useful information for the next assessment step?

A. Autopsy

B. Cuckoo

C. Memdump

D. Nmap

Answer: D

Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

A Cuckoo Sandbox is a tool that is **used to launch malware in a secure and isolated environment**, the idea is the sandbox fools the malware into thinking it has infected a genuine host.

Question #:11

A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

A. Vishing

B. Whaling

C. Phishing

D. Smishing

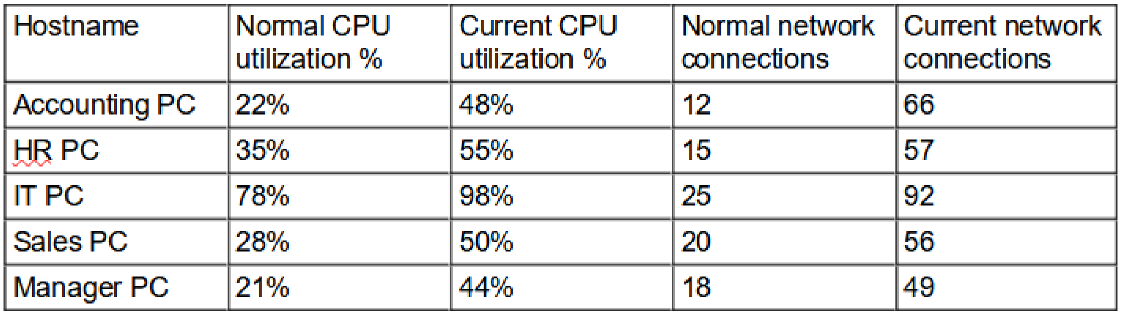
Answer: D

Smishing is phishing via text

Smishing is a phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing. As a variant of phishing, victims are deceived into giving sensitive information to a disguised attacker. SMS phishing can be assisted by malware or fraud websites.

Question #:12

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:



Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting PC	22%	48%	12	66
HR PC	35%	55%	15	57
IT PC	78%	98%	25	92
Sales PC	28%	50%	20	56
Manager PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

A. The ISP is dropping outbound connections

B. The user of the Sales-PC fell for a phishing attack

C. Corporate PCs have been turned into a botnet

D. An on-path attack is taking place between PCs and the router

Answer: C

On-path attackers place themselves between two devices (often a web browser and a web server) and intercept or modify communications between the two.

A botnet attack is **a large-scale cyber attack carried out by malware-infected devices which are controlled remotely**

Question #:13

A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

A. Hoaxes

B. SPIMs

C. Identity fraud

D. Credential harvesting

Answer: A

Explanation

Hoax

A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.

Identity theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.

Credential Harvesting

Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

Question #:14

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports. Which of the following attacks is happening on the corporate network?

A. Man in the middle

B. Evil twin

C. Jamming

D. Rogue access point

E. Disassociation

Answer: B

An Evil twin is made to look like the legitimate network. It uses the same SSID, same network setting, and even same captive portal. It can even at times over power the legitimate access point through a stronger signal, drawing unsuspecting users to input their credentials into it.

Question #:15

An attacker browses a company's online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

A. Hoax

B. Reconnaissance

C. Impersonation

D. pretexting

Answer: B

Reconnaissance: The practice of covertly discovering and collecting information about a system.

Impersonation is a form of social engineering attack when the attacker pretends to be someone else.. nothing related to

that the system is able to respond to changes in demand without encountering performance issues or becoming unavailable.

Question #:16

A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

A. Race-condition

B. Pass-the-hash

C. Buffer overflow

D. XSS

Answer: C

EIP stands for Extended Instruction Pointer and is **used to track the address of the current instruction running inside the application**.

EIP is a register in x86 architectures (32bit). It holds the "Extended Instruction Pointer" for the stack. In other words, it tells the computer where to go next to execute the next command and controls the flow of a program.

A buffer overflow attack is a type of security vulnerability that occurs when a program attempts to write data to a memory buffer that is too small to hold it. This can cause the program to crash or, in some cases, allow an attacker to execute arbitrary code.

One way to identify where the EIP of the stack is located on memory is to use a technique called fuzzing, which involves sending large amounts of data to an application in order to identify areas where the application is vulnerable to buffer overflow attacks

Question #:17

A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

A. internet

B. Screened Subnet

C. VLAN segmentation

D. Zero Trust

Answer: C

Flat network is a computer network design approach that aims to reduce cost, maintenance and administration.

Flat networks are designed to reduce the number of routers and switches on a computer network by connecting the devices to a single switch instead

Networks are typically segmented with VLANs or subnets. VLANs create smaller network segments that connect hosts virtually. Subnets use IP addresses to segment the network, connected by networking devices.

A screened subnet, or triple-homed firewall, refers to a network architecture where a single firewall is used with three network interfaces. It provides additional protection from outside cyber attacks by adding a perimeter network to isolate or separate the internal network from the public-facing internet.

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Question #:18

While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

A. Revoke the code signing certificate used by both programs.

B. Block all unapproved file hashes from installation.

C. Add the accounting application file hash to the allowed list.

D. Update the code signing certificate for the approved application.

Answer: A

Revoke the code signing certificate will prevent the unauthorized program from being executed on the servers, as it will no longer be trusted

Question #:19

A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?

A. Outdated software

B. Weak credentials

C. Lack of encryption

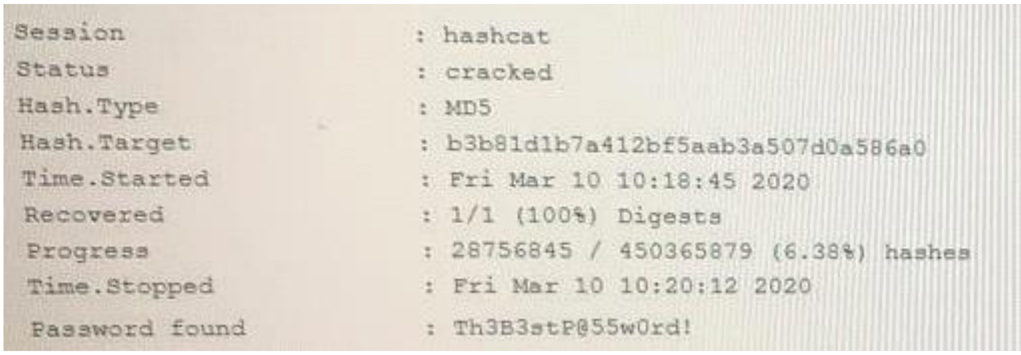
D. Backdoors

Answer: B

Most of the IoT devices have the same password given by the manufacturer.

Question #:20

An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:



```
Session                          : hashcat
Status                           : cracked
Hash.Type                        : MD5
Hash.Target                      : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started                     : Fri Mar 10 10:18:45 2020
Recovered                        : 1/1 (100%) Digests
Progress                         : 28756845 / 450365879 (6.38%) hashes
Time.Stopped                     : Fri Mar 10 10:20:12 2020
Password found                   : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary

B. Pass-the-hash

C. Brute-force

D. Password spraying

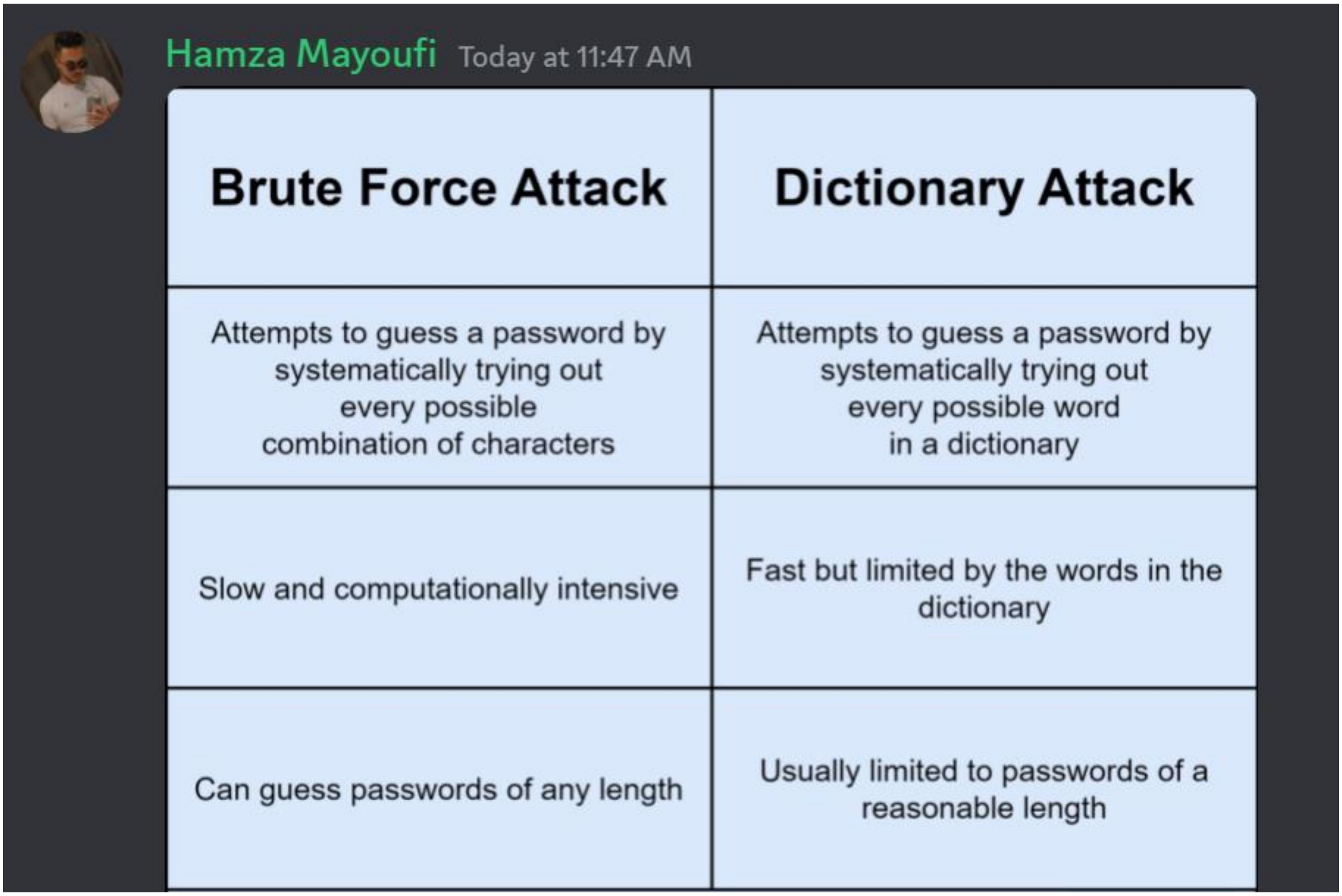
Answer: A

A dictionary attack is a type of password attack where a list of commonly used passwords or words are tried against the target system in an attempt to crack the password hashes. This is often done using a password cracking tool such as hashcat, which is referenced in the logs.

The logs show that the attacker was able to recover a single password hash, and the time it took to crack the password hash suggests that the attack was not done using brute-force, which would have taken much longer.

Password spraying (or, a Password Spray Attack) is when an attacker uses common passwords to attempt to access several accounts on one domain. Using a list of common weak passwords, such as 123456 or password1, an attacker can potentially access hundreds of accounts in one attack.

https://teampassword.com/blog/password-or-p55w0rd



Hamza Mayoufi Today at 11:47 AM

Brute Force Attack	Dictionary Attack
Attempts to guess a password by systematically trying out every possible combination of characters	Attempts to guess a password by systematically trying out every possible word in a dictionary
Slow and computationally intensive	Fast but limited by the words in the dictionary
Can guess passwords of any length	Usually limited to passwords of a reasonable length

Question #:21

While investigating a recent security incident, a security analyst decides to view all network connections on a particular server. Which of the following would provide the desired information?

A. arp

B. nslookup

C. netstat

D. nmap

Answer: C

Netstat: shows all active network connections, network interface information, and ports that are listening. The question is asking to view all the connections on the server which the netstat command will do.

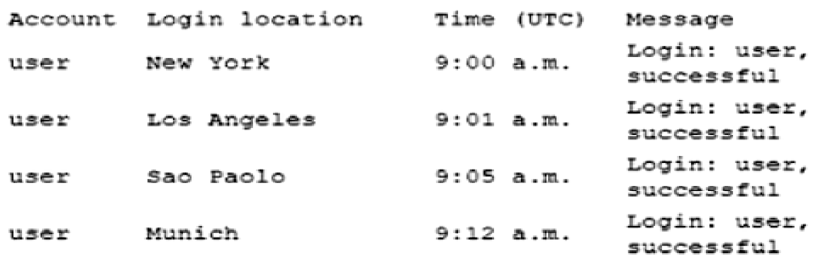
Nmap :a network discovery and security auditing tool mainly used to find services, hosts, and open ports on a network.

Nslookup : queries DNS servers to obtain DNS records

ARP : TCP/IP utility used for viewing and modifying the local Address Resolution Protocol (ARP) cache.

Question #:22

During a recent security incident at a multinational corporation, a security analyst found the following logs for an account called user:



Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paolo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which of the following account policies would BEST prevent attackers from logging in as user?

A. Impossible travel time

B. Geofencing

C. Time-based logins

D. Geolocation

Answer: A

Impossible Travel is a calculation made by comparing a user's last known location to their current location, then assessing whether the trip is likely or even possible in the time that elapsed between the two measurements.

Question #: 23

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports.

B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.

C. Deny unauthenticated users access to shared network folders.

D. Verify computers are set to install monthly operating system updates automatically.

Answer: A

If its' zero day there is no prepared IDS v IPS solutions; hence the most secure to block all SMB traffic might be problematic, but this might be only temporary solution until zero-day stop being zero-day

EDR solution didn't help with the recent attack, thus it will not help with the next attack either, they can not "ensure it" if they could, then why didn't they already do it to prevent the first attack

Going back to what happen in 2017 with WannaCry, and you guys will see that is best practice to disable outbound communication over SMB ports, hence, inbound to ports 137-139, and many EDR solutions out there didn't detect the payloads associated with EternalBlue and DoublePulsar.

Question #: 24

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data

is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

A. Segmentation

B. Containment

C. Geofencing

D. Isolation

Answer: A

Multiprotocol Label Switching, or MPLS, is **a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks**.

Why is MPLS used?

MPLS can be used when speed and reliability are highly important. Applications that require near-immediate data delivery are known as real-time applications. Voice calls and video calls are two common examples of real-time applications. MPLS can also be used to set up wide area networks (WANs).

Question #:25

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing

B. Fuzzing

C. Manual code review

D. Dynamic code analysis

Answer: B

Fuzzing is a type of testing that involves feeding a large number of random and unexpected inputs to a software application to see how it handles the inputs and how it behaves under stress. This testing helps to identify security vulnerabilities and potential problems with the application that could lead to crashes or other issues.

Dynamic code analysis involves testing an application while it is running, looking for potential security vulnerabilities and other problems that could lead to crashes or other issues. This is not the same as testing for unexpected input.

Dynamic code analysis is based on observing how the code behaves during execution. Dynamic analysis is done while a program is in operation and monitors functional behavior and overall performance. Dynamic analysis uses a technique called fuzzing, which enables an attacker to inject random-looking data into a program to see if it can cause the program to crash.

Code signing is **a process by which the software developer signs the applications and executables before releasing them**. It is done by placing a digital signature onto the executable, program, software update or file. The certificate ensures that the software has not been tempered and the user can safely download it.

Emin Gun — Today at 11:52 AM
Fuzz testing or fuzzing is an automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities. A fuzzing tool injects these inputs into the system and then monitors for exceptions such as crashes or information leakage

Question #:26

An enterprise has hired an outside security firm to conduct a penetration test on its network and applications. The enterprise provided the firm with access to a guest account. Which of the following BEST represents the type of testing that is being used?

A. Black-box

B. Red-team

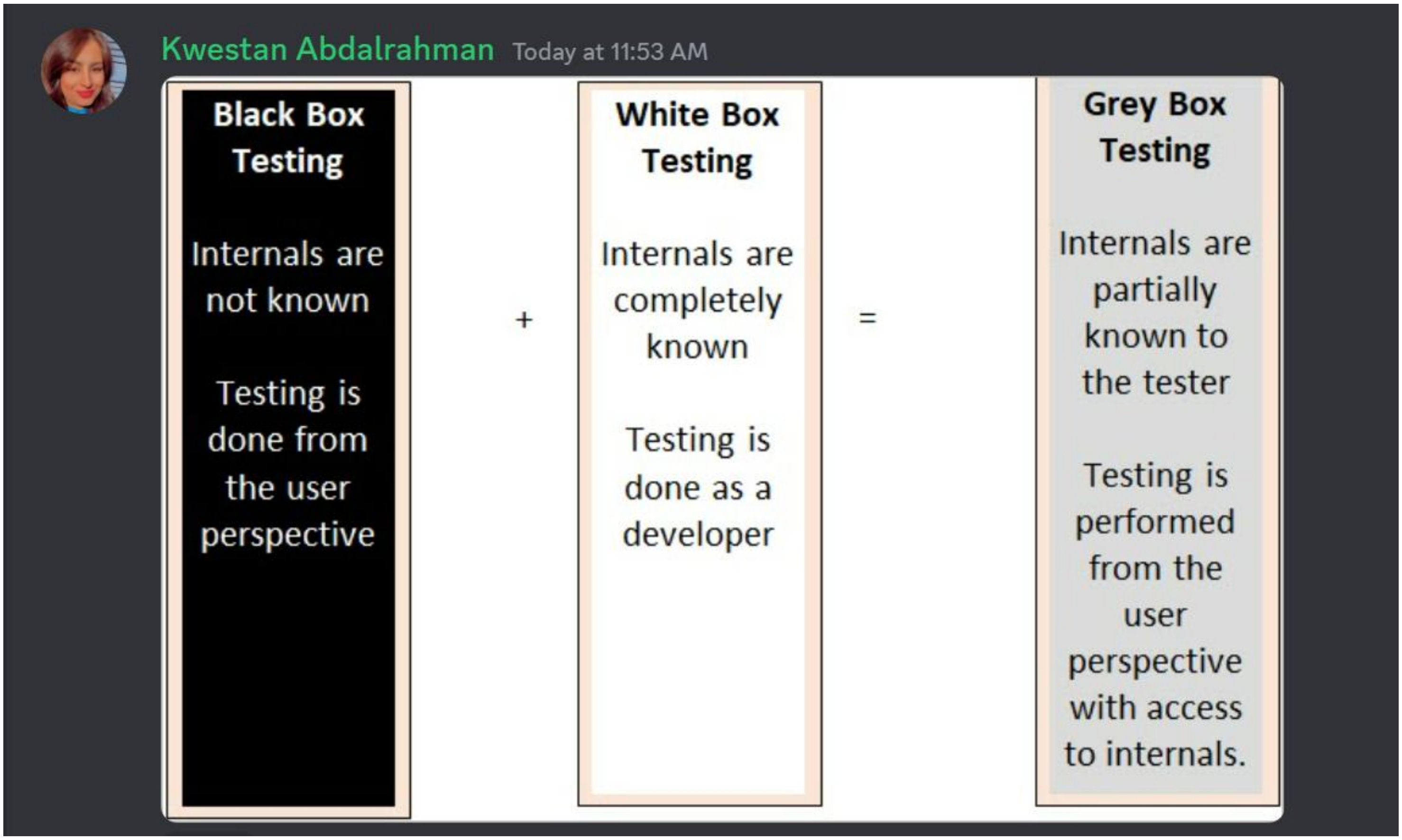
C. Gray-box

D. Bug bounty

E. White-box

Answer: C

Partial knowledge



Kwestan Abdalrahman Today at 11:53 AM

Black Box Testing

Internals are not known

Testing is done from the user perspective

+

White Box Testing

Internals are completely known

Testing is done as a developer

=

Grey Box Testing

Internals are partially known to the tester

Testing is performed from the user perspective with access to internals.

Question #:27

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files(Portable-Executable-32 Files). The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.

B. The workstations are beaconing to a command-and-control server.

C. A logic bomb was executed and is responsible for the data transfers.

D. A fileless virus is spreading in the local network environment

Answer: A

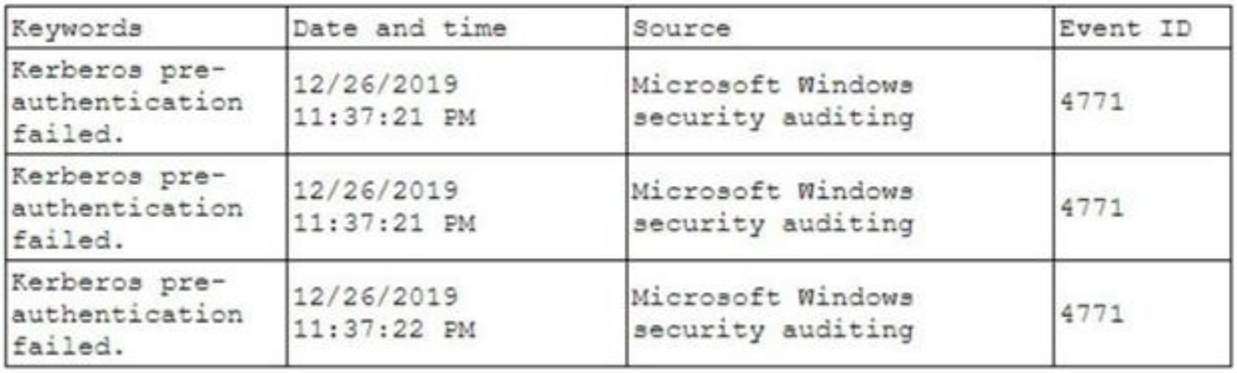
MHT is a web page archive format which stands for MIME HTML.
"A remote access Trojan (RAT) is a type of malware that allows attackers to control systems from remote locations. It is often delivered via drive-by downloads or malicious attachments in email. Once installed on a system, attackers can then access the infected computer at any time and install additional malware if desired.

A growing trend is for attackers to deliver trojans as Portable Executable (PE) files in 32-bit (PE32) and 64-bit (PE64) formats. They often compress the PE files using compression tools, such as tar (sometimes called tarball). Tar files have the .tar.gz file extension."

Jeyhun Shahmardanov — Today at 11:57 AM
A TAR.GZ file is a combination of two different packaging algorithms. The first is tar, short for tape archive. It's an old utility, invented mainly for accurate data transfer to devices without their own file systems. A tar file (or tarball) contains files in a sequential format, along with metadata about the directory structure and other technical parameters.

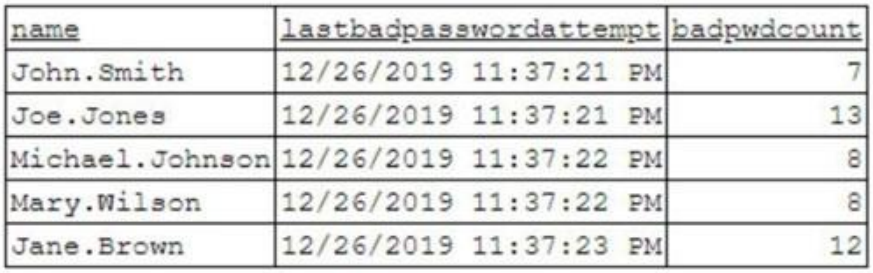
Question #:28

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:



Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:



name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting

B. Keylogger

C. Brute-force

D. Spraying

Answer: D

The timing also indicates password spraying

Brute forcing focuses intensively on one account with every computable password attempt, whereas spraying simply attempts a few or several passwords on an account before moving on.

A ***Password Spraying Attack*** is a type of brute-force attack where a malicious actor attempts the same password on many accounts.

Question #:29

A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps

B. The syslog server

C. The application logs

D. The log retention policy

Answer: B

syslog server receives, categorizes, and stores log messages for analysis, maintaining a comprehensive view of what is going on everywhere on the network. Without this view, devices can malfunction unexpectedly, and outages can be hard to trace.

Question #:30

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.

B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.

C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.

D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

With a CYOD plan, your IT team will have full control of the mobile devices that your employees use. Why would the IT team choose devices that are less secure to begin with? This is not BYOD where the employee has complete control of that decision.

A. incorrect, there cannot be a "common" configuration profile applied to different vendor devices, each device vendor will need a different profile configured for it.

B. incorrect, SCEP-based is the most common type of enrollment, if this were true, all MDM certificates would unnecessarily be exposed.

C. correct, the compensating control would be a baseline mdm profile for each vendor (IOS, Android, Samsung, etc.)

D. incorrect, MDMs do in fact support heterogeneous deployments, minimum most MDM's will support IOS and Android.

Question #:31

During an internal penetration test, a security analyst identified a network device that had accepted cleartext authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device?

A. Configure SNMPv1.

B. Configure SNMPv2.

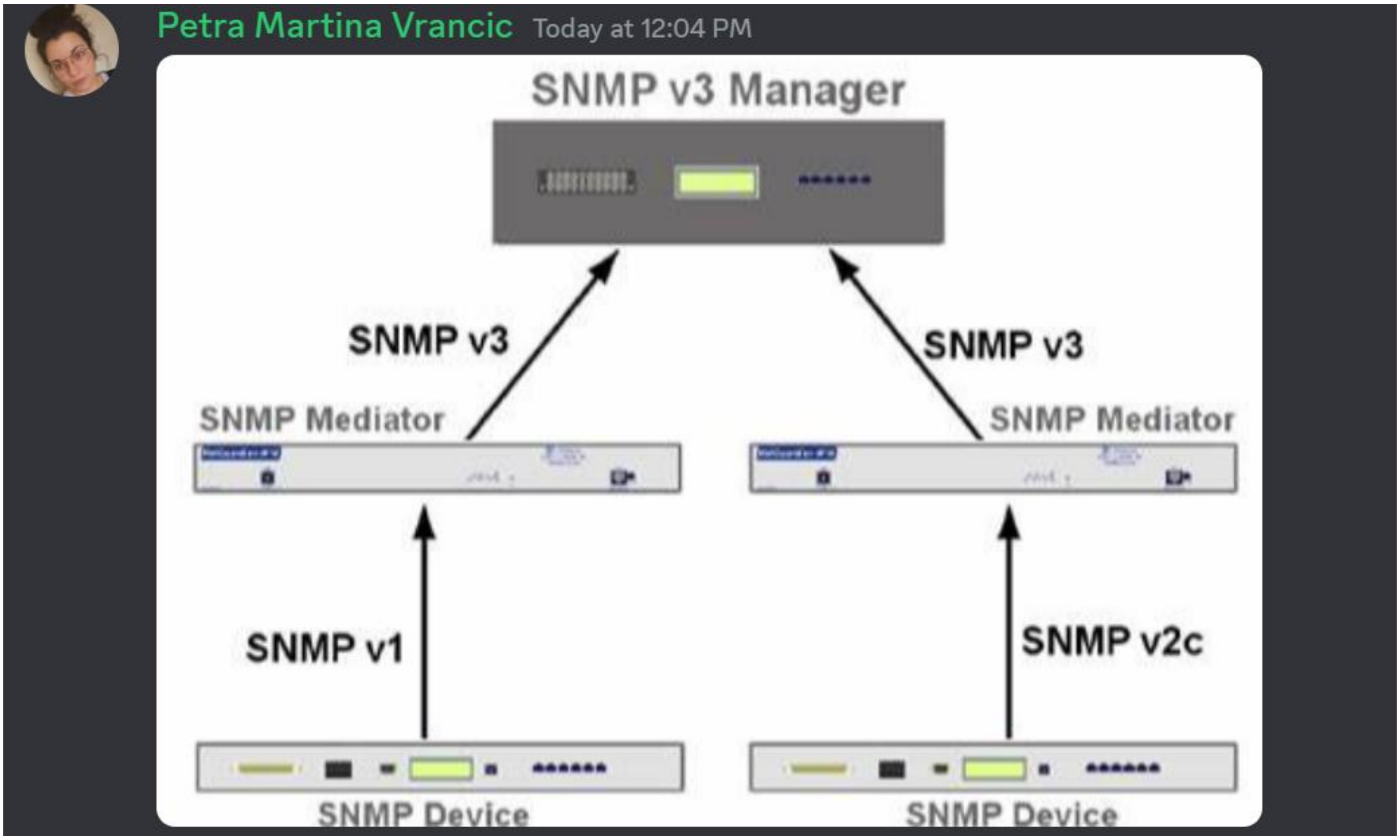
C. Configure SNMPv3.

D. Configure the default community string. // the name of the device 256 char

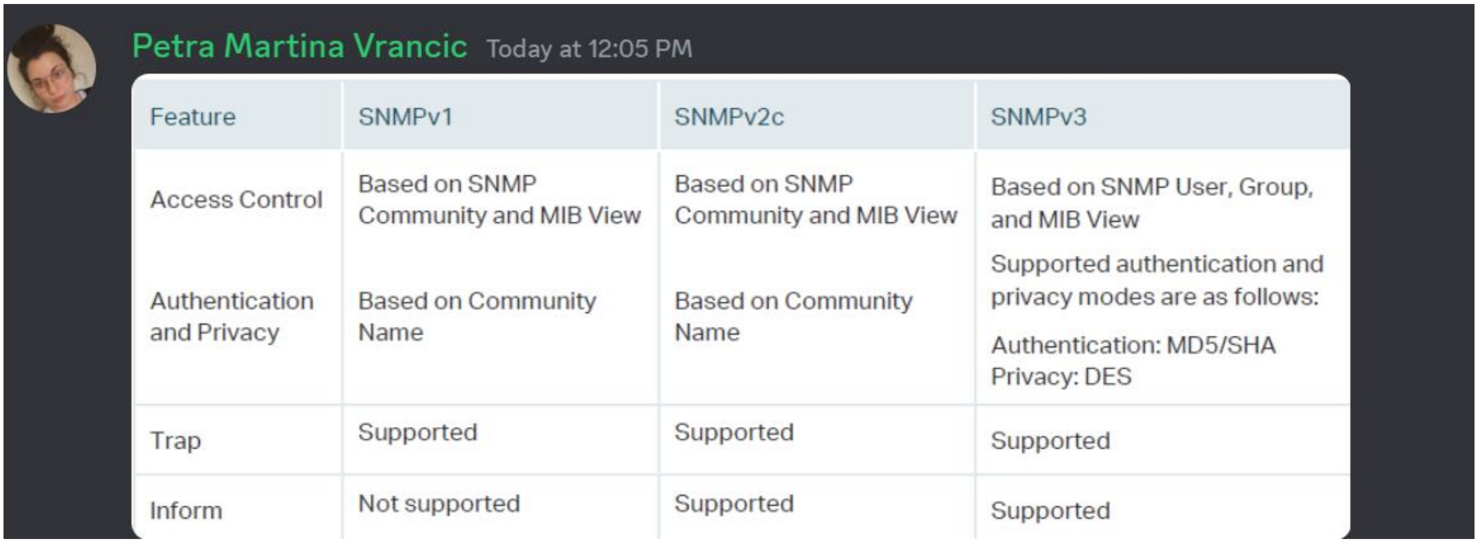
Answer: C

Both SNMPv1 and SNMPv2c provide only simple authentication and do not address encryption. SNMPv2 should only be used in private networks where security is not a major concern. However, the best option is to simply avoid it. Unlike SNMPv1 and SNMPv2c, **SNMP version 3 supports authentication and encryption**.

A device will usually feature a default SNMP community string, which is dependent on the vendor responsible for the device. Some vendors use the word “public” as the default, so **it's crucial users change the default community string to maintain device and network security**.



Petra Martina Vrancic Today at 12:04 PM



Petra Martina Vrancic Today at 12:05 PM

Feature	SNMPv1	SNMPv2c	SNMPv3
Access Control	Based on SNMP Community and MIB View	Based on SNMP Community and MIB View	Based on SNMP User, Group, and MIB View
Authentication and Privacy	Based on Community Name	Based on Community Name	Supported authentication and privacy modes are as follows: Authentication: MD5/SHA Privacy: DES
Trap	Supported	Supported	Supported
Inform	Not supported	Supported	Supported

Question #:32

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner

B. The data processor

C. The data steward

D. The data privacy officer.

Answer: C

A data steward is a job role that is responsible for managing and ensuring the quality of data within an organization. The data steward is typically responsible for defining and implementing data quality standards, policies, and procedures to ensure that data is accurate, complete, and consistent with regulatory and business requirements.

Data owners are responsible for the strategic management of data assets within an organization, including data governance and data management policies. Data processors are responsible for processing data in accordance with established policies and procedures.

Data privacy officers are responsible for ensuring that an organization's data privacy policies and procedures comply with relevant regulations and standards. While they may be involved in data quality and data entry initiatives, their primary focus is on data privacy and security.

Answer: A

Open Web Application Security Project (FRAMEWORK) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. The Open Web Application Security Project provides free and open resources.

Question #:33

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer

B. The data processor

C. The data owner

D. The data controller

Answer: D

In GDPR and other privacy laws, **the data controller** is most responsible for protecting the privacy of and rights to the data. According to Article 5 from the EU GDPR, the controller is responsible for the lawfulness, fairness and transparency of information.

Data Owner — a senior (executive) role with ultimate responsibility for maintaining confidentiality, integrity and availability of the information asset. The owner is responsible for labeling the asset (such as determine who should have access and determine the criticality and sensitivity of the asset) and ensure that it is protected with appropriate controls (access control, backup, retention, and so on). The owner also typically selects an administrator and guardian and directs their actions and sets the budget and allocation of resources for sufficient controls.

Umer Under the GDPR:Data Controller – Is a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it. Data Processor – Is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a data controller.https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

Question #:34

A user recently sent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Answer: D

Sms phishing

Abdullhamit: Spam over internet messaging

Question #:35

An organization’s help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning

B. Domain hijacking

C. Distributed denial-of-service

D. DNS tunneling

Answer: A

ipconfig /flushdns: Flushing DNS will **clear any IP addresses or other DNS records from cache**. This can help resolve security, internet connectivity, and other issues.

When the analyst changed it manually it worked.

The ipconfig /flushdns purges the DNS Resolver Cache. This flushes and resets the contents of the DNS client resolver cache. It can be used during DNS troubleshooting to discard negative cache entries. However, resetting the cache does not eliminate entries that are preloaded from the local Hosts file.

The security analyst changed the DNS to a different server and the issue was resolved. Therefore, the cache was poisoned on the original DNS server.

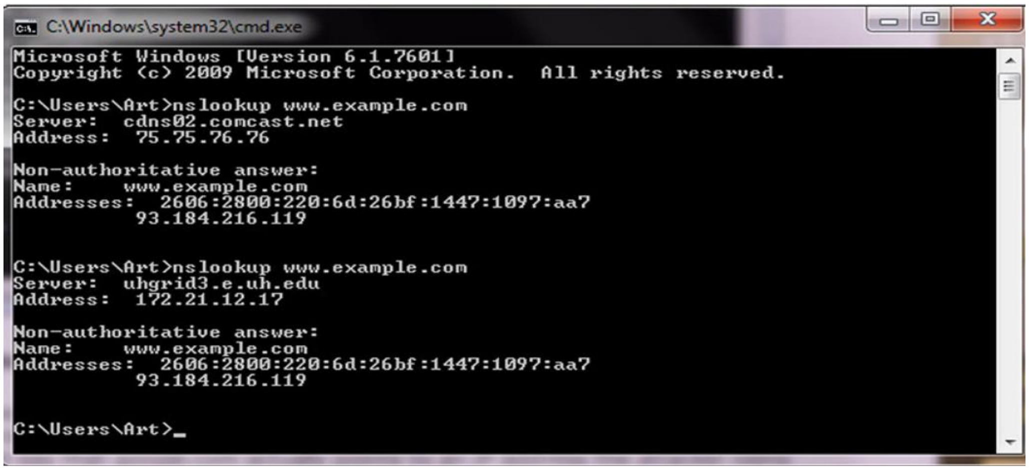
Domain Hijacking or Domain Spoofing is **an attack where an organization's web address is stolen by another party**. The other party changes the enrollment of another's domain name without the consent of its legitimate owner.

DNS hijacking and DNS cache poisoning are both different types of DNS attacks. In DNS hijacking, threat actors subvert DNS resolution by physically taking over DNS settings. But in DNS cache poisoning, threat actors corrupt the DNS cache.

Domain Name Server (DNS) hijacking, also named DNS redirection, is **a type of DNS attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites**.

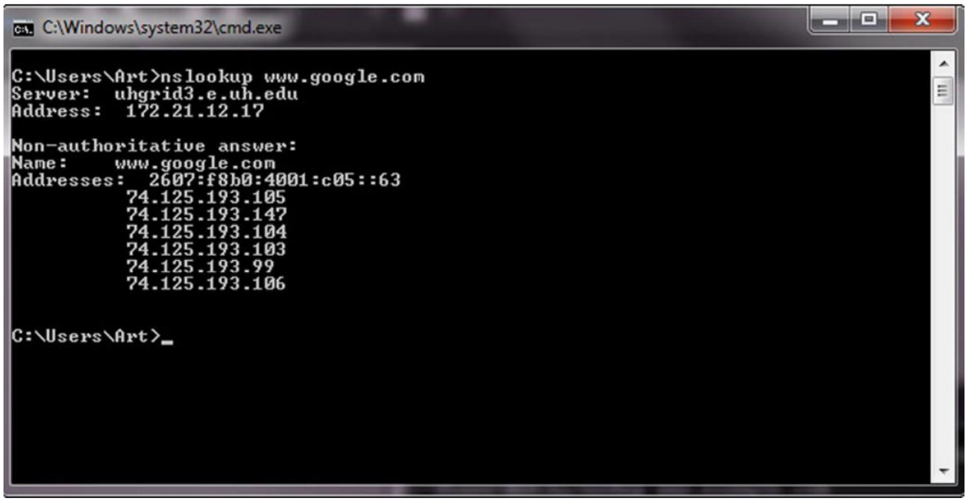
Domain Hijacking Domain hijacking is the act of changing the registration of a domain name without the permission of its original registrant. Technically a crime, this act can have devastating consequences because the DNS system will spread the false domain location far and wide automatically. The original owner can request it to be corrected, but this can take time.

DNS Poisoning: The Domain Name System (DNS) is used to convert a name into an IP address. There is not a single DNS system but rather a hierarchy of DNS servers—from root servers on the backbone of the Internet, to copies at your ISP, your home router, and your local machine, each in the form of a DNS cache. To examine a DNS query for a specific address, you can use the nslookup command. Figure 4-2 shows a series of DNS queries executed on a Windows machine. In the first request, the DNS server was from an ISP, while in the second request, the DNS server was from a virtual private network (VPN) connection. Between the two requests, the network connections were changed, resulting in different DNS lookups. The changing of where DNS is resolved can be a DNS poisoning attack. The challenge in detecting these attacks is knowing what the authoritative DNS entry should be and then detecting when it changes in an unauthorized fashion. Using a VPN can change a DNS source, and this may be desired, but unauthorized changes can be attacks.



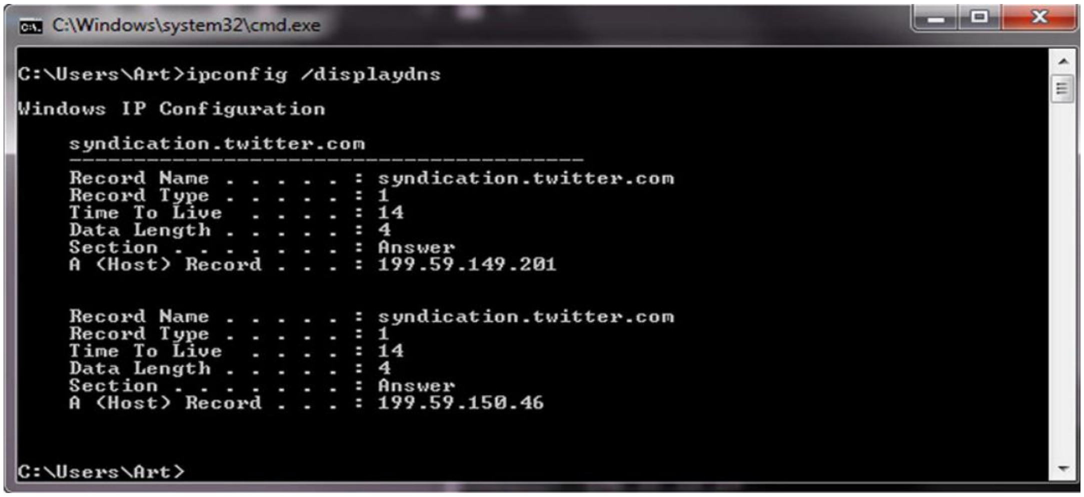
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Art>nslookup www.example.com
Server:  cdns02.comcast.net
Address:  75.75.76.76

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:220:6d:26bf:1447:1097:aa7
          93.184.216.119


C:\Users\Art>nslookup www.example.com
Server:  uhgrid3.e.uh.edu
Address:  172.21.12.17

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:220:6d:26bf:1447:1097:aa7
          93.184.216.119


C:\Users\Art>_
```

At times, nslookup will return a nonauthoritative answer, as shown in Figure 4-3. This typically means the result is from a cache as opposed to a server that has an authoritative answer (that is, an answer known to be current).



```
C:\Users\Art>nslookup www.google.com
Server:  uhgrid3.e.uh.edu
Address:  172.21.12.17

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4001:c05::63
          74.125.193.105
          74.125.193.147
          74.125.193.104
          74.125.193.103
          74.125.193.99
          74.125.193.106


C:\Users\Art>_
```

There are other commands you can use to examine and manipulate the DNS cache on a system. In Windows, the ipconfig /displaydns command will show the current DNS cache on a machine. Figure 4-4 shows a small DNS cache. This cache was recently emptied using the ipconfig /flushdns command to make it fit on the screen.



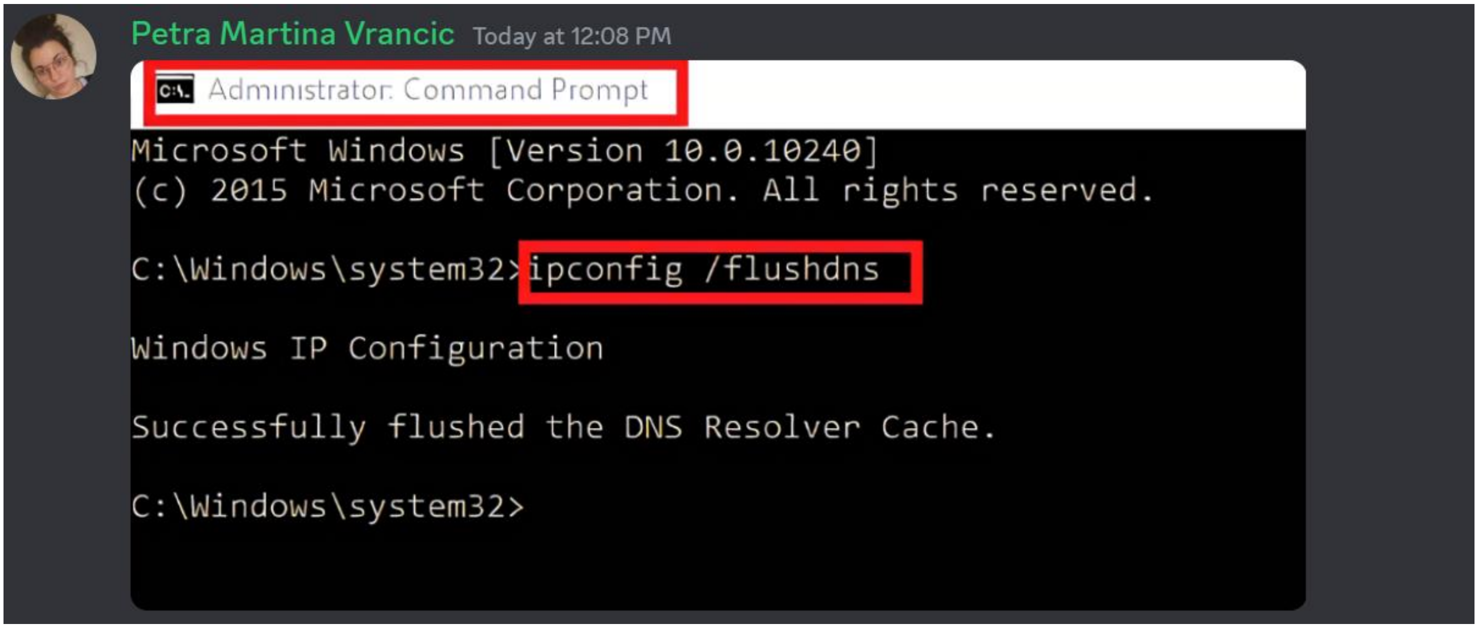
```
C:\Users\Art>ipconfig /displaydns

Windows IP Configuration

    syndication.twitter.com
    ----------------------------------------
    Record Name . . . . . : syndication.twitter.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 14
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 199.59.149.201


    Record Name . . . . . : syndication.twitter.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 14
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 199.59.150.46


C:\Users\Art>
```

Looking at DNS as a complete system shows that there are hierarchical levels from the top (root server) down to the cache in an individual machine. DNS poisoning can occur at any of these levels, with the effect of the poisoning growing wider the higher up it occurs.

In 2010, a DNS poisoning event resulted in the “Great Firewall of China” censoring Internet traffic in the United States until caches were resolved.

DNS poisoning is a variant of a larger attack class referred to as DNS spoofing. In DNS spoofing, an attacker changes a DNS record through any of a multitude of means. There are many ways to perform DNS spoofing, a few of which include compromising a DNS server, the use of the Kaminsky attack, and the use of a false network node advertising a false DNS address. An attacker can even use DNS cache poisoning to result in DNS spoofing.

By poisoning an upstream DNS cache, all of the downstream users will get spoofed DNS records.


Petra Martina Vrancic Today at 12:08 PM

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>
```

Question #:36

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAP are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

Answer: A

Question #: 37

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head

B. Tcpdump

C. grep

D. tail

E. curl

F. openssl

G. dd

Answer: A C

A - "analyst needs to review the first transactions quickly"

C - "search the entire series of requests for a particular string"

Simple Object Access Protocol (SOAP) is **a lightweight XML-based protocol that is used for the exchange of information in decentralized, distributed application environments**. You can transmit SOAP messages in any way that the applications require, as long as both the client and the server use the same method.

Question #: 38

A user contacts the help desk to report the following:

Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

The user was able to access the Internet, but had trouble accessing the department share until the next day.

The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point

B. Evil twin

C. DNS poisoning

D. ARP poisoning

Answer: B

An Evil Twin IS a rouge access point but a rouge access point isn't necessarily malicious. Since this user obviously had their creds stolen, it was an evil twin and the attacker was capturing all their traffic.

The person started seeing fraudulent bank activity after connecting to the wireless network. On top of that a rogue access point would most likely NOT have the same SSID as the corporate network.

Rogue Access Points that are detected during scanning of an organizations network should be classified. If malicious, the Rogue Access Point should be detected and removed from the environment. An administrator should not allow employees to install access points without their authorization.

A regular scan of Wi-Fi access points will also help local network administrators to make sure that nobody has plugged in an access point without permission and detect unauthorized or rogue access points. Another mitigation step is to install network access control on all devices that require authentication for everybody that wants to use any resources on the network.

Question #:39

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. Black-box

C. Gray-box

D. White-box

Answer: B

The firm has only been given the documentation available to the customers of the applications.

Pentests and bug bounty programs *allow testing web platforms by simulating attacks to detect and fix vulnerabilities*.

This is a Cisco CyberOps associate question

Hamida A bug bounty program provides a means for ethical hackers to test an organization's website, mobile app, or software for security vulnerabilities.

Question #:40

Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data

B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data

C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data

D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

Data Owner : a senior (executive) role with ultimate responsibility for maintaining confidentiality, integrity and availability of the information asset. The owner is responsible for labeling the asset (such as determine who should have access and determine the criticality and sensitivity of the asset) and ensure that it is protected with appropriate controls (access control, backup, retention, and so on). The owner also typically selects an administrator and guardian and directs their actions and sets the budget and allocation of resources for sufficient controls.

Data custodian: role includes responsibilities for protecting data, including securing, monitoring, and controlling access to it, as well as ensuring data is accurate, complete, and accessible when needed. Ensuring that backups are properly maintained would fall under the responsibilities of a data custodian, as they would be responsible for protecting data and ensuring its availability.

Question #:41

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap

B. Wireshark

C. Autopsy

D. DNSEnum

Answer: A

Question #:42

During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file?

A. ls

B. chflags

C. chmod

D. lsof

E. setuid

Answer: C

The analyst can use the ‘chmod’ command to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file. The ‘chmod’ command allows the analyst to specify the permissions for the file's owner, group, and others, as well as set or remove special permissions such as set-user-ID and set-group-ID. The syntax for ‘chmod’ is as follows:

chmod [OPTIONS] MODE FILE

where MODE specifies the desired permissions and FILE is the file to modify. For example, to remove the set-user-ID bit and give the owner read and write permissions, the analyst could run the following command:

chmod u+rwx,go-rwx,u-s FILE

ls: command is used to list the files in a directory,

Chflags: is used to change file flags,

lsof : is used to list open files,

setuid: a bit that makes an executable run with the privileges of the owner of the file.

Question #:43

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

A. NIC teaming

B. High availability

C. Dual power supply

D. laaS

Answer: B

Question #:44

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. Payment Card Industry Data Security Standard

B. Cloud Security Alliance Best Practices

C. ISO/IEC 27032 Cybersecurity Guidelines

D. General Data Protection Regulation

Answer: D

The GDPR is a comprehensive data protection regulation that applies to companies that process personal data of individuals in the EU, regardless of the company's location. The GDPR imposes strict requirements on how organizations should handle personal data, including the requirements for obtaining consent, providing transparency in data processing, implementing appropriate security measures, and reporting data breaches.

ISO/IEC 27032 Cybersecurity Guidelines provide a general framework for managing cybersecurity risks, but do not specifically address the management of personal data or compliance with international data protection laws.

Question #: 45

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX

B. CIRT

C. OSINT

D. TAXII

Answer: D

What is TAXII used for?

What is Trusted Automated eXchange of Indicator (TAXII)? Trusted Automated eXchange of Indicator is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII (Trusted Automated Exchange of Indicator Information) often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data. TAXII provides a secure and standardized way for organizations to exchange cyber threat information, such as indicators of compromise, in real-time to enhance their ability to detect and respond to potential cyber attacks.

- Structured Threat Information eXpression (STIX) – Describes cyber threat information – Includes motivations, abilities, capabilities, and response information

- Trusted Automated eXchange of Indicator Information (TAXII) – Securely shares STIX data

Where STIX provides the syntax for describing CTI, the Trusted Automated eXchange of Indicator Information (TAXII) protocol provides a means for transmitting CTI data between servers and clients. For example, a CTI service provider would maintain a repository of CTI data. Subscribers to the service obtain updates to the data to load into analysis tools over TAXII. This data can be requested by the client (referred to as a collection), or the data can be pushed to subscribers (referred to as a channel).

Question #:46

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan

C. A business continuity plan

D. A disaster recovery plan

Answer: B

To inform the affected parties about the compromise of their sensitive data, the organization should use a communications plan. A communications plan outlines how the organization will communicate with stakeholders in the event of a security incident or breach, including affected parties, customers, employees, and the media.

The communications plan should include the following information:

1. Who will be responsible for communicating the incident to the affected parties.

2. What information will be communicated, such as the type of data that was compromised and what actions the organization is taking to address the issue.

3. When and how the information will be communicated, such as through email, phone calls, or a public announcement.

4. How the organization will handle follow-up inquiries and concerns from affected parties.

An incident response plan, business continuity plan, and disaster recovery plan are also important plans for an organization to have, but they are not specifically designed for communicating with affected parties about a security incident or breach.

The Diamond Model is a framework used for intrusion analysis and threat intelligence that helps analysts to organize information about threats and attacks. The model is based on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, analysts can build a better understanding of the threat actors and their tactics, techniques, and procedures (TTPs).

Question #:47

A Chief Information Security Officer has defined resiliency requirements for a new data center architecture. The requirements are as follows:

• Critical file shares will remain accessible during and after a natural disaster. //Geographic dispersal

• Five percent of hard disks can fail at any given time without impacting the data. //RAID

• Systems will be forced to shutdown gracefully when battery levels are below 20%. //UPS

Which of the following are required to BEST meet these objectives? (Select THREE)

A. Fiber switching

B. laC

C. NAS

D. RAID

E. UPS

F. Redundant power supplies

G. Geographic dispersal

H. Snapshots

I. Load balancing

Answer: D E G

D. RAID: Using RAID (Redundant Array of Independent Disks) technology allows for data to be distributed across multiple disks, providing protection against disk failures.

E. UPS: Using an uninterruptible power supply (UPS) will ensure that systems can shut down gracefully when battery levels are low, protecting against data loss due to sudden power outages.

G. Geographic dispersal: Spreading critical data across multiple data centers in different geographic locations will ensure that it remains accessible even if one data center is affected by a natural disaster.

Question #:48

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Answer: B

A USB data blocker, is a device that allows you to plug into USB charging ports including charging kiosks, and USB ports on gadgets owned by other people.

The main purpose of using one is to eliminate the risk of infecting your phone or tablet with malware, and even prevent hackers to install/execute any malicious code to access your data.

Question #: 49

Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

A. Common Weakness Enumeration

B. OSINT

C. Dark web

D. Vulnerability databases

Question #:50

In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

A. Authority

B. Intimidation

C. Consensus

D. Scarcity

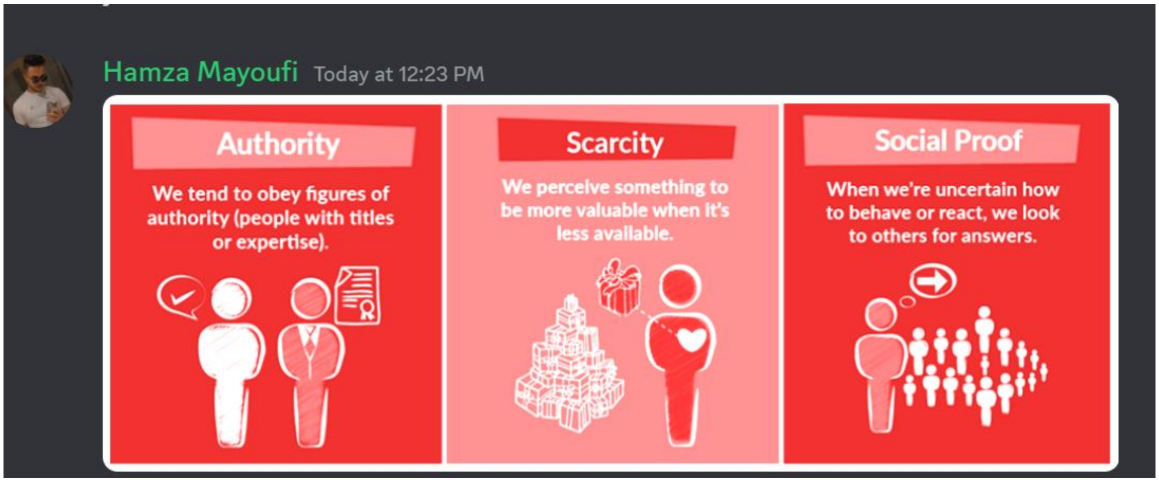
Answer: A

The Psychology of Social Engineering – Why It Works

1. **Reciprocity – People tend to return a favor, thus the pervasiveness of free samples in marketing.**
2. **Commitment and Consistency – If people commit, orally or in writing, to an idea or goal, they are more likely to honor that commitment because they have stated that that idea or goal fits their self-image. Even if the original incentive or motivation is removed after they have already agreed, they will continue to honor the agreement.**
3. **Social Proof – People will do things that they see other people are doing.**
4. **Authority – People will tend to obey authority figures, even if they are asked to perform objectionable acts.**
5. **Liking – People are easily persuaded by other people whom they like.**
6. **Scarcity – Perceived scarcity will generate demand. For example, saying offers are available for a "limited time only" encourages sales.**

Social Engineers are aware of these human biases and take advantage of them in a variety of ways. Social Engineering attacks commonly involve:

- **Pretexting: Masquerading as someone else**
- **Baiting: Enticing the victim with promises of something of value**
- **Blackmail: Threatening to reveal something that the target wishes to be kept secret**
- **Quid Pro Quo (a variant of Baiting): Promising something to the victim in exchange for their help**



Hamza Mayoufi Today at 12:23 PM

Authority

We tend to obey figures of authority (people with titles or expertise).

Scarcity

We perceive something to be more valuable when it's less available.

Social Proof

When we're uncertain how to behave or react, we look to others for answers.

Question #:51

Which of the following control types fixes a previously identified issue and mitigates a risk?

A. Detective

B. Corrective

C. Preventative

D. Finalized

Answer: B

Question #:51

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption

B. Data masking

C. Anonymization

D. Tokenization

Answer: B

Alicia: Homomorphic will process the data while its encrypted

Encryption: Data at rest

Because tokenized data cannot be returned to its original form as its irreversible.
Masking is best when data still in use, while Tokenization and encryptions work best when the data is at rest.
.

Question #:52

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2

B. PCI DSS

C. GDPR

D. ISO 31000

Answer: C

The General Data Protection Regulation (GDPR): comprehensive data protection regulation that sets out rules on how personal data should be processed and protected in the European Union (EU). It establishes the roles and responsibilities of both data controllers and data processors, defines the conditions for lawful processing of personal data, and sets out the rights of data subjects

A: Statement on Standards for Attestation Engagements (SSAE) is a standard from the American Institute of Certified Public Accountants (AICPA). The organization's Auditing Standards Board (ASB) created these regulations to evaluate service companies. SSAE includes three types of reports that review different aspects of a company's operations. The Service and Organization Controls (SOC) 2 report focuses on security and privacy.

B: PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards for organizations that handle credit cards.

D: ISO 31000 Risk Management framework is an international standard that provides businesses with guidelines and principles for risk management from the International Organization for Standardization.

What is the difference between SOC 2 and GDPR?

SOC 2 compliant companies have to inform customers about which data is collected and for what purposes. GDPR compliant companies have to obtain consent for the collection of customer data (especially if this data is being used beyond its original purpose).

Does SOC 2 cover GDPR?

While SOC2 Privacy criteria and the GDPR Regulation both aim at protecting the privacy of Personal Data, it is important to understand that neither of the two are replaceable in place of the other. This means **being SOC2 Compliant cannot completely rule out the need for GDPR**.

Question #:53

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger

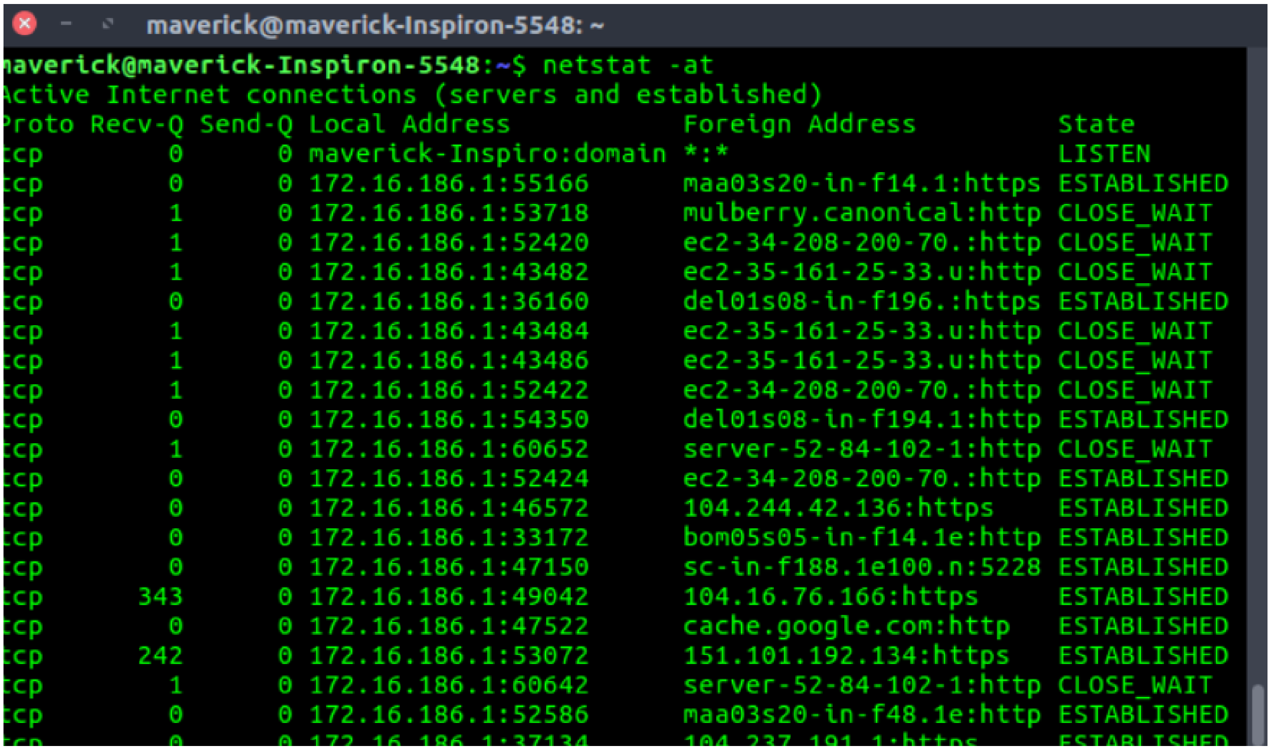
B. Metasploit

C. tcpdump

D. netstat

Answer: D

Netstat



```
averick@maverick-Inspiron-5548:~$ netstat -at
ctive Internet connections (servers and established)
roto Recv-Q Send-Q Local Address           Foreign Address         State
cp        0      0 maverick-Inspiro:domain *:*                     LISTEN
cp        0      0 172.16.186.1:55166      maa03s20-in-f14.1:https ESTABLISHED
cp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
cp        1      0 172.16.186.1:52420      ec2-34-208-200-70.:http CLOSE_WAIT
cp        1      0 172.16.186.1:43482      ec2-35-161-25-33.u:http CLOSE_WAIT
cp        0      0 172.16.186.1:36160      del01s08-in-f196.:https ESTABLISHED
cp        1      0 172.16.186.1:43484      ec2-35-161-25-33.u:http CLOSE_WAIT
cp        1      0 172.16.186.1:43486      ec2-35-161-25-33.u:http CLOSE_WAIT
cp        1      0 172.16.186.1:52422      ec2-34-208-200-70.:http CLOSE_WAIT
cp        0      0 172.16.186.1:54350      del01s08-in-f194.1:http ESTABLISHED
cp        1      0 172.16.186.1:60652      server-52-84-102-1:http CLOSE_WAIT
cp        0      0 172.16.186.1:52424      ec2-34-208-200-70.:http ESTABLISHED
cp        0      0 172.16.186.1:46572      104.244.42.136:https    ESTABLISHED
cp        0      0 172.16.186.1:33172      bom05s05-in-f14.1e:http ESTABLISHED
cp        0      0 172.16.186.1:47150      sc-in-f188.1e100.n:5228 ESTABLISHED
cp      343      0 172.16.186.1:49042      104.16.76.166:https     ESTABLISHED
cp        0      0 172.16.186.1:47522      cache.google.com:http   ESTABLISHED
cp      242      0 172.16.186.1:53072      151.101.192.134:https   ESTABLISHED
cp        1      0 172.16.186.1:60642      server-52-84-102-1:http CLOSE_WAIT
cp        0      0 172.16.186.1:52586      maa03s20-in-f48.1e:http ESTABLISHED
cp        0      0 172.16.186.1:37134      104.237.191.1:https     ESTABLISHED
```