Question 1:
Which of the following USB tools using to copy files from USB devices silently?

- **USBSnoopy**
- **USBGrabber**
- **USBDumper**
- **USBSniffer**

Explanation
https://www.ghacks.net/2006/09/15/how-to-dump-all-usb-files-without-the-user-knowing/

USBdumper runs silently as a background process once started and copies the complete contents of every connected usb device to the system without the knowledge of the user. It creates a directory with the current date and begins the background copying process. The user has no indication that the files stored on the USB device are copied from the USB to the local system.

Question 2:
Identify the encryption algorithm by the description:

Symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 × 32-bit S-boxes based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a "masking" key and a "rotation" key for performing its functions.

- **CAST-128**
- **DES**
- **GOST**
- **AES**

Explanation
https://www.rfc-editor.org/rfc/rfc2144

CAST-128 (alternatively CAST5) is a symmetric-key block cipher used in a number of products, notably as the default cipher in some versions of GPG and PGP. It has also been approved for Government of Canada use by the Communications Security Establishment.

CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 and 128 bits (but only in 8-bit increments). The full 16 rounds are used when the key size is longer than 80 bits.

Components include large 8×32-bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations. There are three alternating types of round function, but they are similar in structure and differ only in the choice of the exact operation (addition, subtraction or XOR) at various points.

CAST-128 uses a pair of subkeys per round: a 32-bit quantity Km is used as a "masking" key and a 5-bit quantity Kr is used as a "rotation" key.

Incorrect answers:

AES https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of

ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

DES https://en.wikipedia.org/wiki/Data_Encryption_Standard

DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure. DES has 16 rounds.

GOST https://en.wikipedia.org/wiki/GOST_(block_cipher)

The GOST block cipher (Magma), defined in the standard GOST 28147-89 (RFC 5830), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The original standard, published in 1989, did not give the cipher any name, but the most recent revision of the standard, GOST R 34.12-2015 (RFC 7801, RFC 8891), specifies that it may be referred to as Magma. The GOST hash function is based on this cipher. The new standard also specifies a new 128-bit block cipher called Kuznyechik.

Question 3:
You need to increase the security of keys used for encryption and authentication. For these purposes, you decide to use a technique to enter an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Which of the following techniques will you use?

- **KDF**
- **PKI**
- **Key reinstallation**
- **Key stretching**

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

Key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking, and key stretching is intended to make such attacks more difficult by complicating a basic step of trying a single password candidate. Key stretching also improves security in some real-world applications where the key length has been constrained, by mimicking a longer key length from the perspective of a brute-force attacker.

There are several ways to perform key stretching. One way is to apply a cryptographic hash function or a block cipher repeatedly in a loop. For example, in applications where the key is used for a cipher, the key schedule in the cipher may be modified so that it takes a specific length of time to perform. Another way is to use cryptographic hash functions that have large memory requirements – these can be effective in frustrating attacks by memory-bound adversaries.

Key stretching algorithms depend on an algorithm that receives an input key and then expends considerable effort to generate a stretched cipher (called an enhanced key[citation needed]) mimicking randomness and longer key length. The algorithm must have no known shortcut, so the most efficient way to relate the input and cipher is to repeat the key stretching algorithm itself. This compels brute-force attackers to expend the same effort for each attempt. If this added effort compares to a brute-force key search of all keys with a certain key length, then the input key may be described as stretched by that same length.

Key stretching leaves an attacker with two options:

- Attempt possible combinations of the enhanced key, but this is infeasible if the enhanced key is sufficiently long and unpredictable (i.e., the algorithm mimics randomness well enough that the attacker must trial the entire stretched key space).

- Attempt possible combinations of the weaker initial key, potentially commencing with a dictionary attack if the initial key is a password or passphrase, but the attacker's added effort for each trial could render the attack uneconomic should the costlier computation and memory consumption outweigh the expected profit.

If the attacker uses the same class of hardware as the user, each guess will take the similar amount of time to process as it took the user (for example, one second). Even if the attacker has much greater computing resources than the user, the key stretching will still slow the attacker down while not seriously affecting the usability of the system for any legitimate user. This is because the user's computer only has to compute the stretching function once upon the user entering their password, whereas the attacker must compute it for every guess in the attack.

This process does not alter the original key-space entropy. The key stretching algorithm is deterministic, allowing a weak input to always generate the same enhanced key, but therefore limiting the enhanced key to no more possible combinations than the input key space. Consequently, this attack remains vulnerable if unprotected against certain time-memory tradeoffs such as developing rainbow tables to target multiple instances of the enhanced key space in parallel (effectively a shortcut to repeating the algorithm). For this reason, key stretching is often combined with salting.

Incorrect answers:

KDF https://en.wikipedia.org/wiki/Key_derivation_function

Key derivation function (KDF) is a cryptographic hash function that derives one or more secret keys from a secret value such as the main key, a password, or a passphrase using a pseudorandom function. KDFs can be used to stretch keys into longer keys or to obtain keys of a required format, such as converting a group element that is the result of a Diffie–Hellman key exchange into a symmetric key for use with AES. Keyed cryptographic hash functions are popular examples of pseudorandom functions used for key derivation.

PKI https://en.wikipedia.org/wiki/Public_key_infrastructure

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity

of the parties involved in the communication and to validate the information being transferred.

In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision. When done over a network, this requires using a secure certificate enrollment or certificate management protocol such as CMP.

Key reinstallation 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.

The weakness is exhibited in the Wi-Fi standard itself, and not due to errors in the implementation of a sound standard by individual products or implementations. Therefore, any correct implementation of WPA2 is likely to be vulnerable. The vulnerability affects all major software platforms, including Microsoft Windows, macOS, iOS, Android, Linux, OpenBSD and others.

The security protocol protecting many Wi-Fi devices can essentially be bypassed, potentially allowing an attacker to intercept sent and received data.

Question 4:
John, a black hacker, is trying to do an SMTP enumeration. What useful information can John gather during a Simple Mail Transfer Protocol enumeration?

- **He can receive a list of all mail proxy server addresses used by the company.**
- **He can find information about the daily outgoing message limits before mailboxes are locked.**
- **He can use the internal command RCPT provides a list of ports open.**
- **He can use two internal commands VRFY and EXPN, which provide information about valid users, email addresses, etc.**

Explanation
https://info-savvy.com/what-is-enumeration/

SMTP is a service that can be found in most infrastructure penetration tests. This service can help the penetration tester to perform username enumeration via the EXPN and VRFY commands if these commands have not been disabled by the system administrator.

The role of the EXPN command is to reveal the actual address of users aliases and lists of email and VRFY which can confirm the existence of names of valid users.

The SMTP enumeration can be performed manually through utilities like telnet and netcat or automatically via a variety of tools like metasploit, nmap and smtp-user-enum.

Question 5:
Identify the correct sequence of steps involved in the vulnerability-management life cycle.

- **Vulnerability scan -> Risk assessment -> Identify assets and create a baseline -> Remediation -> Monitor -> Verification.**

- **Remediation -> Monitor -> Verification -> Vulnerability scan -> Risk assessment -> Identify assets and create a baseline.**
- **Vulnerability scan -> Identify assets and create a baseline -> Risk assessment -> Remediation -> Verification -> Monitor.**
- **Identify assets and create a baseline -> Vulnerability scan -> Risk assessment -> Remediation -> Verification -> Monitor.**

Explanation
According to EC-Council courseware, the correct order is as follows:

1. Identify assets and create a baseline

This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management.

2. Vulnerability scan

This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure.

3. Risk assessment

In this phase, all profound uncertainties associated with the system are assessed and prioritized, and remediation is planned to eliminate system flaws permanently. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets.

4. Remediation

Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

5. Verification

In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets.

6. Monitor

Organizations need to perform regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.

Question 6:
Which term from the following describes a set of vulnerabilities that allows spyware to be installed on smartphones with the iOS operating system, allowing those who conducted espionage to track and monitor every action on the device?

- **Androrat**
- **DroidSheep**
- **Trident**
- **Zscaler**

Explanation
https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf

In August 2016, Lookout, in conjunction with Citizen Lab, discovered “Pegasus,” a sophisticated piece of mobile spyware used by nation state actors to surveil high-value targets.

https://blog.lookout.com/trident-pegasus

“Pegasus is the most sophisticated attack we’ve seen on any endpoint because it takes advantage of how integrated mobile devices are in our lives and the combination of features only available on mobile — always connected (WiFi, 3G/4G), voice communications, camera, email, messaging, GPS, passwords, and contact lists. It is modular to allow for customization and uses strong encryption to evade detection. Lookout’s analysis determined that the malware exploits three zero-day vulnerabilities, or Trident, in Apple iOS:

· **CVE-2016-4655:** Information leak in Kernel - A kernel base mapping vulnerability that leaks information to the attacker allowing him to calculate the kernel’s location in memory.

· **CVE-2016-4656**: Kernel Memory corruption leads to Jailbreak - 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to silently jailbreak the device and install surveillance software.

· **CVE-2016-4657:** Memory Corruption in Webkit - A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.

The attack sequence, boiled down, is a classic phishing scheme: send text message, open web browser, load page, exploit vulnerabilities, install persistent software to gather information. This, however, happens invisibly and silently, such that victims do not know they’ve been compromised.

In this case, the software is highly configurable: depending on the country of use and feature sets purchased by the user, the spyware capabilities include accessing messages, calls, emails, logs, and more from apps including Gmail, Facebook, Skype, WhatsApp, Viber, FaceTime, Calendar, Line, Mail.Ru, WeChat, SS, Tango, and others. The kit appears to persist even when the device software is updated and can update itself to easily replace exploits if they become obsolete.

We believe that this spyware has been in the wild for a significant amount of time based on some of the indicators within the code (e.g., a kernel mapping table that has values all the way back to iOS 7). It is also being used to attack high-value targets for multiple purposes, including high-level corporate espionage on iOS, Android, and Blackberry. “

NOTE: On August 25, Apple released iOS 9.3.5 to address these vulnerabilities

Incorrect answers:

DroidSheep https://droidsheep.info/

This is an open-source Android application made by Corsin Camichel that allows you to intercept unprotected web-browser sessions using WiFi.

Androrat https://github.com/karma9874/AndroRAT

AndroRAT is a contraction of Android and RAT (Remote Access Tool) - a tool designed to give the control of the android system remotely and retrieve information from it.

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

This is an American cloud-based information security company headquartered in San Jose, California.

Question 7:
Ivan, a black hat hacker, got the username from the target environment. In conditions of limited time, he decides to use a list of common passwords, which he will pass as an argument to the hacking tool. Which of the following is the method of attack that Ivan uses?

- **Dictionary attack.**
- **Password spraying attack.**
- **Known plaintext attack.**
- **Smudge attack.**

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

A dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase ***by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords***, often from lists obtained from past security breaches.

A dictionary attack is based on trying all the strings in a pre-arranged listing. Such attacks originally used words found in a dictionary (hence the phrase dictionary attack); however, now there are much larger lists available on the open Internet containing hundreds of millions of passwords recovered from past data breaches. ***There is also cracking software that can use such lists and produce common variations, such as substituting numbers for similar-looking letters***. A dictionary attack tries only those possibilities which are deemed most likely to succeed. Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords; or variants obtained, for example, by appending a digit or punctuation character. Dictionary attacks are often successful since many commonly used password creation techniques are covered by the available lists, combined with cracking software pattern generation. A safer approach is to randomly generate a long password (15 letters or more) or a multiword passphrase, using a password manager program or manually typing a password.

Below you will find several tools that can use this type of attack:

John the Ripper: https://en.wikipedia.org/wiki/John_the_Ripper

Aircrack-ng: https://ophcrack.sourceforge.io/

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

Incorrect answers:

Known plaintext attack https://en.wikipedia.org/wiki/Known-plaintext_attack

The known-plaintext attack (KPA) is a type of cryptanalysis in which standard pieces are present in the ciphertext, the meaning of which is known to the analyst in advance. During the Second World War, English cryptanalysts called such pieces "hints".

Smudge attack https://en.wikipedia.org/wiki/Smudge_attack

A smudge attack is an information extraction attack that discerns the password input of a touchscreen device such as a cell phone or tablet computer from fingerprint smudges. A team of researchers at the University of Pennsylvania were the first to investigate this type of attack in 2010. An attack occurs when an unauthorized user is in possession or is nearby the device of interest. The attacker relies on detecting the oily smudges produced and left behind by the user's fingers to find the pattern or code needed to access the device and its contents. Simple cameras, lights, fingerprint powder, and image processing software can be used to capture the fingerprint deposits created when the user unlocks their device. Under proper lighting and camera settings, the finger smudges can be easily detected, and the heaviest smudges can be used to infer the most frequent input swipes or taps from the user.

Password spraying attack

Password spraying is a type of brute force attack. In this attack, an attacker will brute force ***logins based on list of usernames with default passwords on the application***. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

Question 8:
Your boss has instructed you to introduce a hybrid encryption software program into a web application to secure email messages. You are planning to use free software that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

Which of the following meets these requirements?

- **GPG**
- **S/MIME**
- **SMTP**
- **PGP**

Explanation
GPG https://en.wikipedia.org/wiki/GNU_Privacy_Guard

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a versatile key management system, along with access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command-line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. GnuPG also provides support for S/MIME and Secure Shell (ssh).

GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

Incorrect answers:

SMTP https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

The Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP

to send and receive mail messages. User-level email clients typically use SMTP only for sending messages to a mail server for relaying, and typically submit an outgoing email to the mail server on port 587 or 465 per RFC 8314. For retrieving messages, IMAP (which replaced the older POP3) is standard, but proprietary servers also often implement proprietary protocols, e.g., Exchange ActiveSync.

PGP https://en.wikipedia.org/wiki/Pretty_Good_Privacy

NOTE: *Incorrect because PGP is a proprietary solution owned by Symantec, but the question asked about "free software."*

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 and similar software follow the OpenPGP, an open standard of PGP encryption software, standard (RFC 4880) for encrypting and decrypting data.

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. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include options through an automated key management server.

S/MIME https://en.wikipedia.org/wiki/S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most importantly RFC 3369, 3370, 3850 and 3851. It was originally developed by RSA Data Security and the original specification used the IETF MIME specification with the de facto industry standard PKCS#7 secure message format. Change control to S/MIME has since been vested in the IETF and the specification is now layered on Cryptographic Message Syntax (CMS), an IETF specification that is identical in most respects with PKCS #7. S/MIME functionality is built into the majority of modern email software and interoperates between them. Since it is built on CMS, MIME can also hold an advanced digital signature.

Question 9:
In which of the following attacks does the attacker receive information from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy?

- **Spearphone attack**
- **Smudge attack**
- **DroidDream**
- **SIM swap scam**

Explanation
http://www.winlab.rutgers.edu/~yychen/papers/(WiSec'21)%20Spearphone%20a%20lightweight%20speech%20privacy%20exploit%20via%20accelerometer-sensed%20reverberations%20from%20smartphone%20loudspeakers.pdf

The Spearphone attack breaches speech privacy by exploiting the motion sensor ‘accelerometer’ and capturing speech reverberations generated through the loudspeaker.

This, in turn, empowers the attackers to listen to every sound coming out of the loudspeaker including conversations, music, or any other audio.

Incorrect answers:

Smudge attack https://en.wikipedia.org/wiki/Smudge_attack

A smudge attack is an information extraction attack that discerns the password input of a touchscreen device such as a cell phone or tablet computer from fingerprint smudges. An attack occurs when an unauthorized user is in possession or is nearby the device of interest. The attacker relies on detecting the oily smudges produced and left behind by the user's fingers to find the pattern or code needed to access the device and its contents. Simple cameras, lights, fingerprint powder, and image processing software can be used to capture the fingerprint deposits created when the user unlocks their device. Under proper lighting and camera settings, the finger smudges can be easily detected, and the heaviest smudges can be used to infer the most frequent input swipes or taps from the user.

DroidDream

DroidDream is a mobile botnet type of malware that appeared in spring 2011. The DroidDream Trojan gained root access to Google Android mobile devices in order to access unique identification information for the phone. Once compromised, a DroidDream-infected phone could also download additional malicious programs without the user s knowledge as well as open the phone up to control by hackers.

SIM swap scam https://en.wikipedia.org/wiki/SIM_swap_scam

A SIM swap scam (also known as a port-out scam, SIM splitting, Smishing, and simjacking, SIM swapping) is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone.

Question 10:
You need to hide the file in the Linux system. Which of the following characters will you type at the beginning of the filename?

- **! (Exclamation mark)**
- **_ (Underscore)**
- **~ (Tilda)**
- **. (Period)**

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

Linux hides files and folders that have a period at the start of their name. To hide a file or folder, rename it and place a period at the start of the filename.

Question 11:
The attacker needs to collect information about his victim - Maria. She is an extrovert who often posts a large amount of private information, photos, and location tags of recently visited places on social networks. Which automated tool should an attacker use to gather information to perform other sophisticated attacks?

- **VisualRoute**
- **Hootsuite**
- **HULK**
- **Ophcrack**

Explanation

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

You can easily find a question on this topic in the exam, so it will be presented in this test, but I absolutely disagree with the EC-Council on this. Hootsuite is a ***social media management platform*** (for auto-posting, trends analyzing, etc.)***.*** It collects information from social networks only about users registered in it (photos, posts, etc.). You can read a little more information about their policies here: https://www.hootsuite.com/legal/privacy

But, in the EC-Council's training materials, you will find the only mention of Hootsuite that refers to the answer to this question:

"Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites."

Incorrect answers:

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

Ophcrack is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. On most computers, ophcrack can crack most passwords within a few minutes.

VisualRoute http://www.visualroute.com/

VisualRoute offers a wide variety of network tools that help users keep one step ahead of network issues such as bottle necks and packet loss/latency issues.

HULK

HULK is a Denial of Service (DoS) tool used to attack web servers by generating unique and obfuscated traffic volumes.

HULK’s generated traffic also bypasses caching engines and hits the server’s direct resource pool.

Question 12:
To collect detailed information about services and applications running on identified open ports, nmap can perform version detection. To do this, various probes are used to receive responses from services and applications. Nmap requests probe information from the target host and analyzes the response, comparing it with known responses for various services, applications, and versions. Which of the options will allow you to run this scan?

- **-sV**
- **-sX**
- **-sF**
- **-sN**

Explanation
https://nmap.org/man/ru/man-version-detection.html

- ***-sV (Version detection)***

Enables version detection, as discussed above. Alternatively, you can use -A, which enables version detection among other things.

- ***-sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)***

These three scan types (even more are possible with the *--scanflags* option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports. Page 65 of RFC 793 says that “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response.” Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: “you are unlikely to get here, but if you do, drop the segment, and return.”

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

- ***Null scan (-sN)***

Does not set any bits (TCP flag header is 0)

- ***FIN scan (-sF)***

Sets just the TCP FIN bit.

- ***Xmas scan (-sX)***

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Question 13:
Alex was assigned to perform a penetration test against a website using Google dorks. He needs to get results with file extensions. Which operator should Alex use to achieve the desired result?

- **filetype:**
- **define:**
- **site:**
- **inurl:**

Explanation
https://ahrefs.com/blog/google-advanced-search-operators/

filetype: Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. **Note:** The “ext:” operator can also be used—the results are identical.

Incorrect answers:

site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain.

inurl: Find pages with a certain word (or words) in the URL. For this example, any results containing the word “apple” in the URL will be returned.

define: A dictionary built into Google, basically. This will display the meaning of a word in a card-like result in the SERPs.

Question 14:
When scanning with Nmap, you found a firewall. Now you need to determine whether it is a stateful or stateless firewall. Which of the following options is best for you to use?

- **-sT**

- **-sM**
- **-sA**
- **-sO**

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

TCP ACK Scan (-sA)

This scan is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the -sA option. Its probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet.

Incorrect answers:

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.

TCP Maimon Scan (-sM) 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.

IP Protocol Scan (-sO) https://nmap.org/book/scan-methods-ip-protocol-scan.html

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the -p option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

Question 15:
The company "Work Town" hired a cybersecurity specialist to perform a vulnerability scan by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. What type of vulnerability assessment should be performed for "Work Town"?

- **Passive assessment.**
- **Internal assessment.**
- **External assessment.**
- **Active assessment.**

Explanation
To answer this question, we will have to look at the EC-Council training materials and look at their classification Types of Vulnerability Assessment.

Passive Assessment

Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities.

Active Assessment

A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network.

External Assessment

The external assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers.

Internal Assessment

An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities.

Question 16:
Which of the following tools is an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server?

- **Netsparker**
- **WebCopier Pro**
- **Infoga**
- **NCollector Studio**

Explanation
https://www.netsparker.com/support/what-is-netsparker/

Netsparker is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications, and web services, and identify security flaws. Netsparker can scan all types of web applications, regardless of the platform or the language with which they are built.

Netsparker is the only online web application security scanner that automatically exploits identified vulnerabilities in a read-only and safe way, in order to confirm identified issues.

It also presents proof of the vulnerability so that you do not need to waste time manually verifying it. For example, in the case of a detected SQL injection vulnerability, it will show the database name as the proof of exploit.

Incorrect answers:

Infoga https://github.com/m4ll0k/Infoga

Infoga is a tool gathering email accounts informations (ip,hostname,country,...) from different public source (search engines, pgp key servers and shodan) and check if emails was leaked using haveibeenpwned.com API.

NCollector Studio

NCollector Studio is an all in one offline browser, website ripper/crawler aimed at home users and professionals needing to download specific files from a website or full websites for offline browsing.

WebCopier Pro

WebCopier Pro allows saving complete copies of your favorite sites, magazines, or stock quotes. Companies can transfer their intranet contents to staff computers, create a copy of companies' online catalogs and brochures for sales personal, backup corporate web sites, print downloaded files.

Question 17:
The attacker knows about a vulnerability in a bare-metal cloud server that can enable him to implant malicious backdoors in firmware. Also, the backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS. What type of cloud attack can be performed by an attacker exploiting the vulnerability discussed in the above scenario?

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

Explanation
https://www.bleepingcomputer.com/news/security/hackers-backdoor-cloud-servers-to-attack-future-customers/

Cloudborne vulnerability can allow attackers to implant backdoor implants in the firmware or BMC of bare-metal servers that survive client reassignment in bare metal and general cloud services, leading to a variety of attack scenarios.

Bare-metal servers can be compromised by potential attackers which could add malicious backdoors and code in the firmware of a server or in its baseboard management controller (BMC) with minimal skills.

"The Baseboard Management Controller (BMC) is a third-party component designed to enable remote management of a server for initial provisioning, operating system reinstall and troubleshooting," says IBM.

Once this type of backdoor implant is successfully dropped on a bare metal server, it will survive between client switches performed by the provider.

As detailed by Eclypsium, "Truly removing a malicious implant could require the service provider to physically connect to chips to reflash the firmware, which is highly impractical at scale."

By exploiting this vulnerability, dubbed Cloudborne, would-be attackers can go through a number of attack scenarios:

- Performing a permanent denial-of-service (PDoS) attack or just bricking the compromised bare metal server

- Stealing or intercepting data from the application running on the cloud service

- Running a ransomware-type of attack by either damaging data on the bare metal server or disabling the application

Incorrect answers:

Man-in-the-cloud (MITC) attack

https://www.imperva.com/docs/hii_man_in_the_cloud_attacks.pdf

"Man-in-the-Cloud" (MITC) attacks rely on common file synchronization services (such as GoogleDrive and Dropbox) as their infrastructure for command and control (C&C), data exfiltration, and remote access. MITC does not require any particular malicious code or exploit to be used in the initial “infection” stage, thus making it very difficult to avoid. Furthermore, the use of well-known synchronization protocols make it extremely difficult (if not impossible) to distinguish malicious traffic from normal traffic. Even if a compromise is suspected, the discovery and analysis of evidence will not be easy, as little indication of the compromise is left behind on the endpoint. In the MITC attacks, the attacker gets access to the victim’s account without compromising the victim’s user name or password.

Metadata spoofing attack

Metadata spoofing is a process of changing or modifying service metadata written in the web service definition language (WSDL) file, where the information regarding service instances is stored. Once the manipulated file is successfully deployed, cloud users are redirected to unknown places, which is similar to the process of DNS spoofing.

Cloud cryptojacking

https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking

Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.

Question 18:
Which of the following is an anonymizer that masks real IP addresses and ensures complete and continuous anonymity for all online activities?

- **https://www.wolframalpha.com**
- **https://karmadecay.com**
- **https://www.guardster.com**
- **https://www.baidu.com**

Explanation
I know that this question looks very strange. However, you may come across a question on this topic on the exam. In order to answer it, it is enough to know which of the following is a service for anonymous surfing.

https://www.guardster.com/

"Guardster offers various services to let you use the Internet anonymously and securely. From our popular free web proxy service, to our secure SSH tunnel proxy, we have a variety of services to suit your needs."

Question 19:
What is the name of the technique in which attackers move around the territory in a moving vehicle and use special equipment and software to search for vulnerable and accessible WiFi networks?

- **Spectrum analysis**
- **Rogue access point**
- **Wardriving**
- **Wireless sniffing**

Explanation
https://us-cert.cisa.gov/ncas/tips/ST05-003

Mobile device + Wireless network card + antenna + GPS access + Special software. This is all that needs to find if not all, most of the vulnerable and accessible wireless Internet networks in your area or even city in just a few hours. Does it sound like a plot from a movie? But this is reality.

Wardriving occurs when someone uses software and hardware to locate unsecured wireless networks and potentially access them. Software applications are needed to figure out passwords and decrypt networks. Hardware includes a mobile device such as a wireless laptop, a GPS system, and a wireless network.

Wardrivers travel around looking for Wi-Fi signals, plotting the Wi-Fi access points on a map — also called access point mapping — and gathering data on those networks. Wardrivers stay on the move, usually in vehicles, to find those Wi-Fi networks along their route. Variations of wardriving include warbiking, warcycling, warwalking, warjogging, warrailing, wartraining, and warkitting.

The legality of wardriving can be confusing. Laws don't expressly prohibit or permit wardriving, but the act may have legal implications under certain jurisdictions and circumstances.

For instance, in the United States, it isn't illegal to gather data on wireless networks. Wardriving can have peaceful purposes like data collection and computer-generated mapping.

But exploiting wardriving could be problematic if a wardriver accesses a private network. Hacking into networks that aren't yours — especially when accessing another person's data and with malintent — could be considered a network attack and deemed criminal activity.

Wardriving can be dangerous on a larger scale when the hack involves corporate networks.

Incorrect answers:

Spectrum analysis https://en.wikipedia.org/wiki/Spectral_density_estimation

Spectrum analysis helps you detect various types of interference, non Wi-Fi interference, or interference that can also be transient in nature that decreases the performance of your wireless network. Spectrum analysis enables you to visualize the radio frequencies operating in your area and determine the strength of the detected signals.

Wireless sniffing

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html

Wireless sniffing is the practice of eavesdropping on communications within a wireless network by using special software or hardware tools. Sniffing is more intrusive than wireless stumbling, which is looking for the presence of wireless networks. The motives behind wireless sniffing can range from troubleshooting to a malicious attack against a network or individual.

Rogue access point https://en.wikipedia.org/wiki/Rogue_access_point

A rogue access point (rogue AP) is any wireless access point that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing unauthorized wireless access to the network's wired infrastructure. Most of the time, rogue APs are set up by employees who want wireless access when none is available.

Question 20:
Storing cryptographic keys carries a particular risk. In cryptography, there is a mechanism in which a third party stores copies of private keys. By using it, you are can ensure that in the case of a catastrophe, be it a security breach, lost or forgotten keys, natural disaster, or otherwise, your critical keys are safe.

What is the name of this mechanism?

- **Key encapsulation**
- **Key schedule**
- **Key escrow**
- **Key whitening**

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

Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.

NOTE: A third party can be not only a person, there are many solutions on the market for depositing keys. For example, in corporate environments, BitLocker escrow keys are stored in Active Directory.

Key escrow system https://csrc.nist.gov/glossary/term/key_escrow_system

The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data.

Incorrect answers:

Key whitening https://en.wikipedia.org/wiki/Key_whitening

It is a technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key.

Key schedule https://en.wikipedia.org/wiki/Key_schedule

In cryptography, the so-called product ciphers are a certain kind of cipher, where the (de-)ciphering of data is typically done as an iteration of rounds. The setup for each round is

generally the same, except for round-specific fixed values called a round constant, and round-specific data derived from the cipher key called a round key. A key schedule is an algorithm that calculates all the round keys from the key.

Key encapsulation https://en.wikipedia.org/wiki/Key_encapsulation

Key encapsulation mechanisms (KEMs) are a class of encryption techniques designed to secure symmetric cryptographic key material for transmission using asymmetric (public-key) algorithms.

Question 21:
Enabling SSI directives allows developers to add dynamic code snippets to static HTML pages without using full-fledged client or server languages. However, suppose the server is incorrectly configured (for example, allowing the exec directive) or the data is not strictly verified. In that case, an attacker can change or enter directives to perform malicious actions.

What kind of known attack are we talking about?

- **Server-side JS injection**
- **Server-side includes injection**
- **Server-side template injection**
- **CRLF injection**

Explanation
https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection

SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. They are similar to CGIs, except that SSIs are used to execute some actions before the current page is loaded or while the page is being visualized. In order to do so, the web server analyzes SSI before supplying the page to the user.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

NOTE: All options are associated with injections. You just need to choose the right technology.

Question 22:
John sends an email to his colleague Angela and wants to ensure that the message will not be changed during the delivery process. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key did John use to encrypt the checksum?

- **His own private key.**
- **Angela's public key.**
- **Angela's private key**
- **His own public key.**

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

Just a little tricky question. You should carefully read the sentence: "He creates a checksum of the message and **encrypts it** using asymmetric cryptography". This means that he is encrypting something for Angela (even checksum), which she can then decrypt using her private key.

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key (which may be known to others) and a private key (which may not be known by anyone 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.

Question 23:
Which of the following is an example of a scareware social engineering attack?

- **A pop-up appears to a user stating, "You have won money! Click here to claim your prize!"**
- **A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."**
- **A banner appears to a user stating, "Your order has been delayed. Click here to find out your new delivery date."**
- **A banner appears to a user stating, "Your password has expired. Click here to update your password."**

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

It's a very simple question, but nevertheless, you may meet a similar one on the exam, so you just have to be ready for it.

Scareware refers to scam tactics and fake software applications that cybercriminals use to incite feelings of panic and fear. They do this to get users to make irrational split-second decisions and to trick them into:

- Buying worthless software;

- Downloading different types of malicious software;

- Visiting websites that auto-download and install malicious software onto their devices.

Scareware scammers use social engineering tactics and language that create a sense of urgency in their targets to compel their targets to act. They frequently rely on pop-ups that are designed to look like antivirus alerts. In some cases, the messages can take over part (or all) of the target’s screen.

In general, scareware messages are associated with fake antivirus software and tech support scams. They falsely notify people that their devices (such as their computer, tablet, mobile phone) are infected with various types of malware.

Question 24:
Which of the following SOAP extensions apply security to Web services and maintain the integrity and confidentiality of messages?

- **WS-Policy**
- **WS-Security**
- **WSDL**
- **WS-BPEL**

Explanation
https://en.wikipedia.org/wiki/WS-Security

Web Services Security (WS-Security, WSS) is an extension to SOAP to apply security to Web services. It is a member of the Web service specifications and was published by OASIS.

The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as Security Assertion Markup Language (SAML), Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.

WS-Security describes three main mechanisms:

- How to sign SOAP messages to assure integrity. Signed messages also provide non-repudiation.

- How to encrypt SOAP messages to assure confidentiality.

- How to attach security tokens to ascertain the sender's identity.

The specification allows a variety of signature formats, encryption algorithms, and multiple trust domains, and is open to various security token models, such as:

- X.509 certificates

- Kerberos tickets

- User ID/Password credentials

- SAML Assertions

- Custom-defined tokens.

Incorrect answers:

WS-Policy https://en.wikipedia.org/wiki/WS-Policy

WS-Policy is a specification that allows web services to use XML to advertise their policies (on security, quality of service, etc.) and for web service consumers to specify their policy requirements.

WS-Policy is a W3C recommendation as of September 2007.

WS-Policy represents a set of specifications that describe the capabilities and constraints of the security (and other business) policies on intermediaries and end points (for example, required security tokens, supported encryption algorithms, and privacy rules) and how to associate policies with services and end points.

WS-BPEL https://en.wikipedia.org/wiki/Business_Process_Execution_Language

The Web Services Business Process Execution Language (WS-BPEL), commonly known as BPEL (Business Process Execution Language), is an OASIS standard executable language for specifying actions within business processes with web services. Processes in BPEL export and import information by using web service interfaces exclusively.

WSDL https://en.wikipedia.org/wiki/Web_Services_Description_Language

The Web Services Description Language (WSDL) is an XML-based interface description language that is used for describing the functionality offered by a web service. The acronym is also used for any specific WSDL description of a web service (also referred to as a WSDL file), which provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns. Therefore, its purpose is roughly similar to that of a type signature in a programming language.

Question 25:
The date and time of the remote host can theoretically be used against some systems to use weak time-based random number generators in other services. Which option in Zenmap will allow you to make ICMP Timestamp ping?

- **-PU**
- **-PN**
- **-PY**
- **-PP**

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

Don't ping

- nmap -PN [target]

UDP ping

- Nmap -PU [target]

ICMP Timestamp ping nmap

- nmap -PP [target]

SCTP Init Ping

- nmap -PY [target]

NOTE: https://nmap.org/zenmap/

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open-source application that aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows the interactive creation of Nmap command lines. Scan results can be saved

and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Question 26:
Alex, a security engineer, needs to determine how much information can be obtained from the firm's public-facing web servers. First of all, he decides to use Netcat to port 80 and receive the following output:

```
1.  HTTP/1.1 200 OK -
2.
3.  Server: Microsoft-IIS/6 -
4.  Expires: Tue, 17 Jan 2011 01:41:33 GMT
5.  Date: Mon, 16 Jan 2011 01:41:33 GMT
6.
7.  Content-Type: text/html -
8.
9.  Accept-Ranges: bytes -
10. Last Modified: Wed, 28 Dec 2010 15:32:21 GMT
11. ETag:"b0aac0542e25c31:89d"
12.
13. Content-Length: 7369 -
```

Which of the following did Alex do?

- **Cross-site scripting.**
- **SQL injection.**
- **Cross-Site Request Forgery.**
- **Banner grabbing.**

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

Banner Grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, Nmap and Netcat.

For example, one could establish a connection to a target web server using Netcat, then send an HTTP request. The response will typically contain information about the service running on the host:

```
[root@prober]# nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix)  (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

Incorrect answers:

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

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

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. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. 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.

Cross-Site Request Forgery 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.

Question 27:
Which of the following is the type of attack that tries to overflow the CAM table?

- **MAC flooding**
- **Evil twin attack**
- **DNS flood**
- **DDoS attack**

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

A CAM overflow attack occurs when an attacker connects to a single or multiple switch ports and then runs a tool that mimics the existence of thousands of random MAC addresses on those switch ports. The switch enters these into the CAM table, and eventually the CAM table fills to capacity. When a switch is in this state, no more new MAC addresses can be learned; therefore, the switch starts to flood any traffic from new hosts out of all ports on the switch.

A CAM overflow attack turns a switch into a hub, which enables the attacker to eavesdrop on a conversation and perform man-in-the-middle attacks.

Incorrect answers:

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

A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade.

Evil twin attack https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

Evil Twin attacks are mainly the Wi-Fi equivalent of phishing scams. An attacker will setup a fake Wi-Fi access point, and users will connect to this rather than a legitimate one. When users connect to this access point, all of the data they share with the network will pass through a server controlled by the attacker.

DNS flood https://en.wikipedia.org/wiki/DNS_Flood

DNS Flood is a type of denial-of-service attack. It is the process whereby the traffic on a network resource or machine is stopped for some time. The offender sends a great number of requests to the resource or machine so that it might become unavailable to those who might try to reach it. During a DNS flood the host that connects to the Internet is disrupted due to an overload of traffic. It can be referred to as a disruption that causes the work of the resource or machine to halt by not allowing the traffic to land on it.

Question 28:
Whois services allow you to get a massive amount of valuable information at the stage of reconnaissance. Depending on the target's location, they receive data from one of the five largest regional Internet registries (RIR). Which of the following RIRs should the Whois service contact if you want to get information about an IP address registered in France?

- **LACNIC**
- **RIPE NCC**
- **ARIN**
- **APNIC**

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

A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number resources include IP addresses and ***autonomous system (AS)*** numbers.

The regional Internet registry system evolved over time, eventually dividing the responsibility for management to a registry for each of five regions of the world. The regional Internet

registries are informally liaised through the unincorporated ***Number Resource Organization (NRO)***, which is a coordinating body to act on matters of global importance.

· American Registry for Internet Numbers (ARIN)

· RIPE Network Coordination Centre (RIPE NCC)

· Asia-Pacific Network Information Centre (APNIC)

· Latin American and Caribbean Network Information Centre (LACNIC)

· African Network Information Centre (AFRINIC)

NOTE: There are also national RIRs https://en.wikipedia.org/wiki/National_Internet_registry

· The Japan Network Information Center (JPNIC)

· The Korea Internet & Security Agency (KISA/KRNIC)

· China Internet Network Information Center (CNNIC)

· Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)

· Taiwan Network Information Center (TWNIC)

· Vietnam Internet Network Information Center (VNNIC)

· Indian Registry for Internet Names and Numbers (IRINN)

Question 29:
Which of the following is the fastest way to perform content enumeration on a web server using the Gobuster tool?

- **Performing content enumeration using the brute-force mode and 10 threads.**

- **Performing content enumeration using the brute-force mode and random file extensions.**
- **Skipping SSL certificate verification.**
- **Performing content enumeration using a wordlist.**

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

https://en.wikipedia.org/wiki/Brute-force_attack

To answer this question, you need to pay attention to the phrase "fastest way", and nothing is said about success. Naturally, a Dictionary attack (a form of brute force attack) will be much "faster" than the common brute-force attack.

Wordlist Specification (Gobuster) https://patchthenet.com/articles/using-gobuster-to-find-hidden-web-content/

Gobuster enumerates directories and files by performing dictionary attacks.

A dictionary attack consists of testing a list of words, (or a combination of words) in the hope that the correct word is contained within this list.

So, in order for Gobuster to perform a dictionary attack, we need to provide it with a wordlist. To do that, just type in the '-w' option, followed by the path to the wordlist file. We can use a file from the wordlists that we've downloaded earlier.

```
gobuster dir -u http://www.targetwebsite.com/ -w /usr/share/wordlists/big.txt
```

Question 30:
What is the name of a popular tool (or rather, an entire integrated platform written in Java) based on a proxy used to assess the security of web applications and conduct practical testing using a variety of built-in tools?

- **Wireshark**
- **Burp Suite**
- **Nmap**
- **CxSAST**

Explanation
https://portswigger.net/burp

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp Suite is installed by default in Kali Linux.

The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. The Community edition has significantly reduced functionality. It intends to provide a comprehensive solution for web application security checks.

The Burp tools you will use for particular tasks are as follows:

· ***Scanner*** - This is used to automatically scan websites for content and security vulnerabilities.

· ***Intruder*** - This allows you to perform customized automated attacks, to carry out all kinds of testing tasks.

· ***Repeater*** - This is used to manually modify and reissue individual HTTP requests over and over.

· ***Collaborator client*** - This is used to generate Burp Collaborator payloads and monitor for resulting out-of-band interactions.

· ***Clickbandit*** - This is used to generate clickjacking exploits against vulnerable applications.

· ***Sequencer*** - This is used to analyze the quality of randomness in an application's session tokens.

· ***Decoder*** - This lets you transform bits of application data using common encoding and decoding schemes.

· ***Comparer*** - This is used to perform a visual comparison of bits of application data to find interesting differences.

Incorrect answers:

Wireshark https://en.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.

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

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

CxSAST https://checkmarx.com/product/cxsast-source-code-scanning/

CxSAST is application performance management software and includes features such as diagnostic tools.

Question 31:
What is the "wget 192.168.0.10 -q -S" command used for?

- **Flooding the web server with requests to perform a DoS attack.**
- **Performing content enumeration on the web server to discover hidden folders.**
- **Using wget to perform banner grabbing on the webserver.**
- **Download all the contents of the web page locally.**

Explanation
https://securitytrails.com/blog/banner-grabbing

Banner Grabbing allows an attacker to discover network hosts and running services with their versions on the open ports and moreover operating systems so that he can exploit the remote host server.

There are many tools for banner grabbing, including wget.

Command:

wget 192.168.0.10 **-q -S**

The -q will suppress the normal output, and the -S parameter will print the headers sent by the HTTP server, which also works for FTP servers.

The result:

```
[test@wgettest ~]# wget 192.168.0.15 -q -S
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Mon, 08 Nov 2021 13:29:13 GMT
Content-Type: text/html
Content-Length: 5683
Last-Modified: Thu, 21 Oct 2021 17:44:09
GMT Connection: keep-alive ETag: "5bb65169-1633"
Accept-Ranges: bytes
[test@wgettest ~]#
```

Question 32:
Identify the type of SQL injection where attacks extend the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

- **Error-based SQL Injection**
- **Union SQL injection**
- **Blind SQL Injection**

Explanation
https://pentest-tools.com/blog/sql-injection-attacks/

UNION-based SQL Injection

The UNION operator extends the results returned by the original query, enabling users to run two or more statements if they have the same structure as the original one.

Incorrect answers:

Blind SQL Injection

Blind SQL Injection attack does not show any error message, hence “blind” in its name. It is more difficult to exploit as it returns information when the application is given SQL payloads that return a true or false response from the server. By observing the response, an attacker can extract sensitive information.

Error-based SQL Injection

Error-based SQL Injection is one of the most common types of SQL Injection vulnerabilities. It is also quite easy to determine. It relies on feeding unexpected commands or invalid input, typically through a user interface, to cause the database server to reply with an error that may contain details about the target: structure, version, operating system, and even to return full query results.

Out-of-band SQL Injection

With Out-of-band SQL Injection, the application shows the same response regardless of the user input and the database error. To retrieve the output, a different transport channel like

HTTP requests or DNS resolution is used; note that the attacker needs to control said HTTP or DNS server.

Question 33:
Adam is a shopaholic, and he constantly surfs on the Internet in search of discounted products. The hacker decided to take advantage of this weakness of Adam and sent a fake email containing a deceptive page link to his social media page with information about a sale. Adam anticipating the benefit didn't notice the malicious link, clicked on them and logged in to that page using his valid credentials. Which of the following tools did the hacker probably use?

- **Evilginx**
- **PyLoris**
- **XOIC**
- **sixnet-tools**

Explanation
During the exam, you will meet several questions where the situation will be described very abstractly, and several tools are given to choose from. You can answer these questions by the exclusion method. One of the options will be correct, and three are absolutely wrong, such as in this question.

Evilginx (https://github.com/kgretzky/evilginx) - Evilginx is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service. It's core runs on Nginx HTTP server, which utilizes proxy_pass and sub_filter to proxy and modify HTTP content, while intercepting traffic between client and server.

XOIC is a DDoS attacking tool.

PyLoris is aslow HTTP DoS tool which enables the attacker to craft its own HTTP request headers.

sixnet-tools is a tool for exploiting sixnet RTUs.

Question 34:
Which of the scenarios corresponds to the behaviour of the attacker from the example below:

The attacker created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

- **Use of command-line interface.**
- **Data staging.**
- **Unspecified proxy activities.**
- **DNS tunnelling.**

Explanation
You will probably find such a classification of Adversarial Behavioral Identification only in the EC-Council's training materials. Still, you can find a question on this topic on the exam, so you need to understand it.

Unspecified Proxy Activities

An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains.

Use of Command-Line Interface

On gaining access to the target system, an adversary can use the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code.

Data staging

After successfully penetrating a target's network, the adversary uses data staging techniques to collect and combine as much data as possible. The types of data collected by an adversary include sensitive data about the employees and customers, financial information, etc.

DNS tunnelling

Adversaries use DNS tunnelling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network. Using DNS tunnelling, an adversary can also communicate with the command and control server, bypass security controls, and perform data exfiltration.

Question 35:
The cyber kill chain is essentially a cybersecurity model created by Lockheed Martin that traces the stages of a cyber-attack, identifies vulnerabilities, and helps security teams to stop the attacks at every stage of the chain. At what stage does the intruder transmit the malware via a phishing email or another medium?

- **Installation**
- **Delivery**
- **Actions on Objective**
- **Weaponization**

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

The cyber kill chain consists of 7 distinct steps:

1. Reconnaissance

The attacker collects data about the target and the tactics for the attack. This includes harvesting email addresses and gathering other information.

2. Weaponization

Attackers develop malware by leveraging security vulnerabilities. Attackers engineer malware based on their needs and the intention of the attack. This process also involves attackers trying to reduce the chances of getting detected by the security solutions that the organization has in place.

3. Delivery

The attacker delivers the weaponized malware via a phishing email or some other medium. The most common delivery vectors for weaponized payloads include websites, removable disks, and emails. This is the most important stage where the attack can be stopped by the security teams.

4. Exploitation

The malicious code is delivered into the organization's system. The perimeter is breached here. And the attackers get the opportunity to exploit the organization's systems by installing tools, running scripts, and modifying security certificates.

5. Installation

A backdoor or remote access trojan is installed by the malware that provides access to the intruder. This is also another important stage where the attack can be stopped using systems such as HIPS (Host-based Intrusion Prevention System).

6. Command and Control

The attacker gains control over the organization's systems and network. Attackers gain access to privileged accounts and attempt brute force attacks, search for credentials, and change permissions to take over the control.

7. Actions on Objective

The attacker finally extracts the data from the system. The objective involves gathering, encrypting, and extracting confidential information from the organization's environment.

Question 36:
The network administrator has received the task to eliminate all unencrypted traffic inside the company's network. During the analysis, it detected unencrypted traffic in port UDP 161. Which of the following protocols uses this port and what actions should the network administrator take to fix this problem?

- **SNMP and he should change it to SNMP V2.**
- **CMIP and enable the encryption for CMIP.**
- **RPC and the best practice is to disable RPC completely.**
- **SNMP and he should change it to SNMP V3.**

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

SNMP operates in the application layer of the Internet protocol suite. All SNMP messages are transported via User Datagram Protocol (UDP). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response is sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162.

SNMPv1 is the oldest and original version of the SNMP protocol, supporting 32-bit counters. SNMP v1 biggest flaw is its use of a clear-text community string, which is used to identify the device and forms a very primitive style of authentication. With most devices using the default community string is "public", there is a significant risk of snooping or unauthorized changes depending on whether permissions have been set to read-only or write.

SNMPv2 was created to alleviate the issue of the 32-bit counters, upgrading the protocol's capabilities to support 64-bit. The risks surrounding the community string still remain.

SNMPv3 was recognized by the IETF in 2004. It adds ***both encryption and authentication options*** to prevent snooping and unauthorized access. Set us is far more complicated than creating a community string but mitigates many of the risks inherent in SNMP v1 and v2c.

Question 37:
Ivan, an evil hacker, spreads Emotet malware through the malicious script in the organization he attacked. After infecting the device, he used Emote to spread the infection across local networks and beyond to compromise as many machines as possible.

He reached this thanks to a tool which is a self-extracting RAR file (containing bypass and service components) to retrieve information related to network resources such as writable share drives.

What tool did Ivan use?

- **NetPass.exe**
- **Outlook scraper**
- **Mail PassView**
- **Credential enumerator**

Explanation
https://cybersecurity.wa.gov/news/emotet-growing-threat

Credential enumerator: a self-extracting RAR file containing two components, a bypass and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet then writes the service component on the system, which writes Emotet onto the disk. Access to SMB can result in entire domains (servers and clients) becoming infected.

Incorrect answers:

NetPass.exe: a legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.

Outlook scraper: a tool that scrapes names and email addresses from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.

Mail PassView: a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail and passes them to the credential enumerator module.

Question 38:
This attack exploits a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. Also, it further allows the transmission of web-service requests and response messages using different TCP connections.

Which of the following attacks matches the description above?

- **WS-Address spoofing**
- **Soap Array Attack**
- **SOAPAction spoofing**
- **XML Flooding**

Explanation
https://www.ws-attacks.org/WS-Addressing_spoofing

The WS-Address standard allows the addition of routing information to the SOAP Header, allowing asynchronous communication.

WS-Address spoofing – Generic

The generic definition describes the following scenario: An attacker send a SOAP message, containing WS-Address information, to a web service server. The <ReplyTo> element doesn't contain the address of the attacker but instead the web service client who the attacker has chosen to receive the message. This results in unwanted traffic/SOAP messages for the receiving web service client. Depending on the amount of traffic DOS scenarios are possible. However other attack scenarios are possible too.

WS-Address spoofing - BPEL Rollback

This subtype requires the existence of some sort of BPEL engine. Lets assume that an attacker sends SOAP messages to a web service resulting in the creation of new BPEL process instances. The SOAP message contains a <ReplyTo> element with an invalid callback endpoint. After the SOAP message gets processed by the BPEL engine, it tries to call the endpoint defined in <ReplyTo>. This action results in some form of error response such as refused connections or SOAP faults. In return, this error response will be processed by the BPEL engine.
In case a BPEL engine gets flooded with many SOAP messages as described above, a high workload for the BPEL engine will result. In the worst case a DOS is the result. This kind of flooding attack is a lot more devastating than regular flooding attacks, since one message results in the call of multiple actions/web service calls that are called by the BPEL engine. The attack only becomes visible once all stages of the BPEL engine are run through.

Incorrect answers:

SOAPAction spoofing https://www.ws-attacks.org/SOAPAction_Spoofing

Each web service request contains some sort of operation that is later executed by the application logic. This operation can be found in the first child element of the SOAP Body. However, if HTTP is used to transport the SOAP message the SOAP standard allows the use of an additional HTTP header element called SOAPAction. This header element contains the name of the executed operation. It is supposed to inform the receiving web service of what operation is contained in the SOAP Body, without having to do any XML parsing.

This "optimisation" can be used by an attacker to mount an attack, since certain web service frameworks determine the operation to be executed solely on the information contained in the SOAPAction attribut.

XML Flooding https://www.ws-attacks.org/XML_Flooding

XML Flooding (also known XML Flood) aims at exhausting the resources of a web service by sending a large number of legitimate SOAP Messages. This attack can be compared to the classical denial of service attack on web servers by flooding them with a large amount of valid HTTP requests until the server is unable to respond.

Soap Array Attack https://www.ws-attacks.org/Soap_Array_Attack

SOAP messages are flexible in many ways, even Arrays are supported. If you are new to SOAP arrays check the documentation by the W3C .

However this feature that can be exploited by an attacker to cause a denial of service attack to limit the web service availability.

Before an SOAP array is used, its size has to be defined, just like with many other programming languages. By default, SOAP doesn't limit the number of elements within an array. This property can be exploited by an attacker to execute a DOS attack limiting the availability of the web service. Let's assume an attacker declares an array with 1,000,000,000 String elements. Before the message is processed any further by the parser, the web service will reserve space for 1,000,000,000 String Elements in the RAM. In most cases that will lead to memory exhaustion of the attacked system.

Question 39:
Identify the type of fault injection attack to IoT device by description:

During this attack attacker injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. Also, an attacker injects faults into the clock network used for delivering a synchronized signal across the chip.

- **Frequency/voltage tampering**
- **Temperature attack**
- **Optical, EMFI, BBI**
- **Power/clock/reset glitching**

Explanation
According to EC-Council's courseware:

Power/Clock/Reset Glitching

These types of attacks occur when faults or glitches are injected into the power supply that can be used for remote execution, also causing the skipping of key instructions. Faults can also be injected into the clock network used for delivering a synchronized Signal across the chip.

Incorrect answers:

Optical, Electromagnetic Fault Injection (EMFI), Body Bias Injection (BBI)

The main objective of these attacks is to inject faults into devices by projecting lasers and electromagnetic pulses that are used in analog blocks such as random number generators (RNGs) and for applying high-voltage pulses. These faults are then used by the attackers in compromising the system's security.

Frequency/Voltage Tampering

In these attacks, the attackers try to tamper with the operating conditions of a chip, and they can also modify the level of the power supply and alter the clock frequency of the chip. The attackers intend to introduce fault behaviour into the chip to compromise the device security.

Temperature Attacks

Attackers alter the temperature for operating the chip, thereby changing the whole operating environment. This attack can be operated in non-nominal conditions.

Question 40:
Identify Google advanced search operator which helps an attacker gather information about websites that are similar to a specified target URL?

- **[inurl:]**
- **[related:]**
- **[link:]**
- **[site:]**

Explanation
https://ktflash.gitbooks.io/ceh_v9/content/222_footprinting_using_advanced_google_hacking_tec.html

[related:] Lists web pages that are similar to a specified web page.

Incorrect answers:

[link:] Lists web pages that have links to the specified web page.

[site:] Restricts the results to those websites in the given domain.

[inurl:] Restricts the results to documents containing the search keyword in the URL.

Question 41:
Identify the wrong answer in terms of Range:

802.11a - 150 ft

802.11b - 150 ft

802.11n - 150 ft

802.16 (WiMax) - 30 miles

- **802.11b**
- **802.11a**
- **802.16**
- **802.11n**

Explanation

Amendments	Range, meters (ft)
802.11 (Wi-Fi)	20-100 (65-328)
802.11a	35-100 (115-328)
	5000 (16 404)
802.11b	35-140 (115-459)
802.11g	38-140 (125-459)
802.11n	70-250 (230-820)
802.16 (WiMAX)	1609.34-9656.06 (1-6 miles)

Question 42:
You need to identify the OS on the attacked machine. You know that TTL: 64 and Window Size: 5840.

Which is OS running on the attacked machine?

- **Linux OS**
- **Mac OS**
- **Google's customized Linux**
- **Windows OS**

Explanation
https://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting

Network traffic from a computer can be analyzed to detect what operating system it is running. This is to a large extent due to differences in how the TCP/IP stack is implemented in various operating systems.

You can inspect the initial Time To Live (TTL) in the IP header and the TCP window size (the size of the receive window) of the first packet in a TCP session, i.e. the SYN or SYN+ACK packet and identify OS using the following table:

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

Question 43:
Which of the following is the best description of The final phase of every successful hacking - Clearing tracks?

- **During a cyberattack, a hacker corrupts the event logs on all machines.**
- **During a cyberattack, a hacker injects a rootkit into a server.**
- **After a system is breached, a hacker creates a backdoor.**
- **A hacker gains access to a server through an exploitable vulnerability.**

Explanation
The final phase of every successful hacking attack is clearing the tracks. It is very important, after gaining access and misusing the network, that the attacker cover the tracks to avoid being traced and caught. To do this, the attacker clears all kinds of logs and malicious malware related to the attack. During this phase, the attacker will disable auditing and clear and manipulate logs.

Question 44:
Ivan, a black hacker, wants to get information about IoT cameras and devices used by the attacked company. For these purposes, he will use a tool that collects information about the IoT devices connected to a network, open ports and services, and the attack surface area.

Thanks to this tool, Ivan constantly monitors every available server and device on the internet. This opportunity will allow him to exploit these devices in the future.

Which of the following tools did Ivan use to carry out this attack?

- **Wapiti**
- **Lacework**
- **NeuVector**
- **Censys**

Explanation

One more question where you must choose the tool according to the abstract description of the situation. You will meet several similar questions on the exam. To correctly answer such questions, you just need to know which tool does what without going into details.

Censys https://censys.io/product/hnri/

Censys provides an automated monitoring solution, integrated with your existing IT work flow, to scan your employees' home networks for exposures and vulnerabilities. The Censys HNRI ASM tool allows you to map your workforce, alerts you when risks are detected, and allows you to investigate changes over time.

The Censys HNRI looking for:

- Exposed IOT and embedded devices, such as cameras and routers;

- Exposed telnet, FTP, and the like - plaintext services found on many IOT devices and home routers - many with default credentials;

- Remote desktop sharing, such as PCAnywhere and RDP;

- Network management exposures, such as Intel AMT and SNMP;

- Exposed Microsoft LAN protocols like SMB - a popular vector for ransomware.

NeuVector https://neuvector.com/

NeuVector delivers Full Lifecycle Container Security with the only cloud-native, Kubernetes security platform providing end-to-end vulnerability management, automated CI/CD pipeline security, and complete run-time security including the industry's only container firewall to protect your infrastructure from zero-days and insider threats.

Lacework https://www.lacework.com/

Lacework is the data-driven security platform for the cloud. The Lacework Cloud Security Platform, powered by Polygraph, automates cloud security at scale so our customers can innovate with speed and safety.

Wapiti https://wapiti.sourceforge.io/

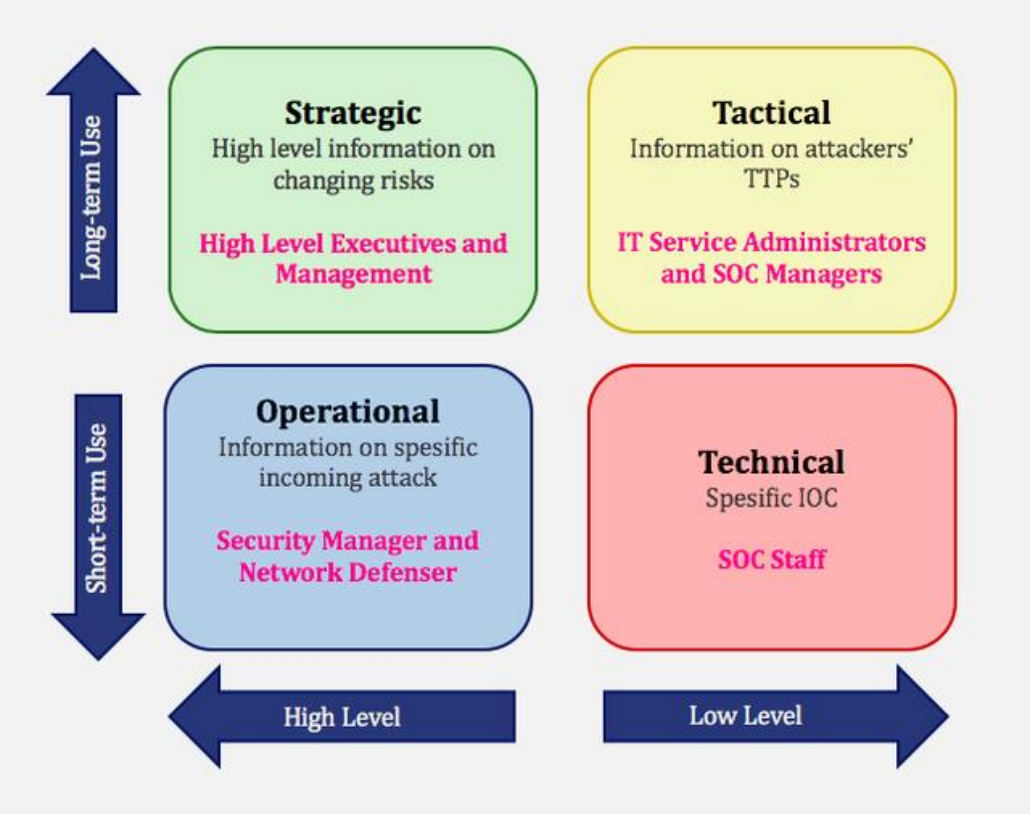
Wapiti allows you to audit the security of your websites or web applications.

It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data.

Question 45:
You need to protect the company's network from imminent threats. To complete this task, you will enter information about threats into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the company's network. Which of the following types of threat intelligence will you use?

- **Tactical threat intelligence.**
- **Strategic threat intelligence.**
- **Operational threat intelligence.**
- **Technical threat intelligence.**

Explanation
https://info-savvy.com/types-of-threat-intelligence/



Technical threat intelligence.

With technical cyber intelligence, information about the attacker's resources such as command and control channel, tools are collected. For example, it focuses on phishing emails or technical tips that indicate the cybersecurity threat to fraudulent URLs. The aim is to collect information about specific IOCs (IP address, phishing email header, hash checksum). This type of threat intelligence is important because it allows to analyze attacks. However, the value of technical threat intelligence is short-lived, as hackers often change their tactics. IOCs that are detected and analyzed at the right time are important. Tactical intelligence is used by employees in the SOC team. Thanks to the information obtained here, new rules are written in the current security products of the organization (such as IDS / IPs, firewall, endpoint security system). Also, suspicious IPs are detected by spam emails. The information obtained here feeds the products of the organization directly.

Incorrect answers:

Strategic threat intelligence

Strategic Threat Intelligence provides a high level of information on the cybersecurity posture, threats, financial impact of cyber activities, attack trends, and their impact on business decisions. The information obtained can be used by senior executives at the company. The purpose of Strategic Threat Intelligence is to manage existing cyber risks and

unknown future risks. This intelligence offers a risk-based approach. It focuses on the effects and possibilities of risks. The information provided here is suitable for long-term use. It helps in making strategic business decisions. For example, it can evaluate these results when deciding on budget / employee / product balance in protecting critical assets. Data collection sources for strategic intelligence are also high-level sources: OSINT, CTI vendors, and ISAO / ISACS.

Operational threat intelligence

Operational threat intelligence provides information to the managers of the defense teams about the specific threat to the company. People like head of network defenders, fraud detection manager incident response team manager understand the attack effect With incoming intelligence, it is attempted to identify the threat actor and to determine his capabilities and threatened IT assets.

In operational threat intelligence, information is collected through hacker forums, chat rooms, social media, and the current cyber attack. The attack that may come with the collected information is estimated, and protection planning is issued.

Tactical threat intelligence

Tactical threat intelligence provides detailed information on the tactics, techniques, and procedures of threat actors. It is predominantly for a technical audience and helps them to understand how their networks are attacked based on the latest methods attackers used to achieve their goals. It provides information that can be consumed by security experts such as IT managers, SOC managers, NOC managers. These employees use tactical cyber intelligence to understand the technical capability and objectives of the offensive and identify their detection and mitigation strategies. Tactical cyber intelligence is collected through malware and incident reports, attack group reports, human Intelligence, and campaign reports.

Question 46:
During testing, you discovered a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as viewing, updating and deleting sensitive data.

Which of the following API vulnerabilities have you found?

- **Code Injections.**
- **No ABAC validation.**
- **Business Logic Flaws.**
- **RBAC Privilege Escalation.**

Explanation
To answer this question, we will use the EC-Council's courseware.

No ABAC validation: No proper attribute-based access control (ABAC) validation allows attackers to gain unauthorized access to API objects or perform actions such as viewing, updating, or deleting.

RBAC Privilege Escalation: Privilege escalation is a common vulnerability present in APIs having role-based access control (RBAC) where changes to endpoints are made without proper attention. Allow attackers to gain access to users' sensitive information

Business Logic Flaws: Many APIs come with vulnerabilities in business logic. Allow attackers to exploit legitimate workflows for malicious purposes.

Code Injections: If the input is not sanitized, attackers may use code injection techniques such as SQLi and XS5 to add malicious SQL statements or code to the input fields on the API. Allow attackers to steal critical information such as session cookies and user credentials.

Question 47:
Which of the following algorithms is a symmetric key block cipher with a block size of 128 bits representing a 32-round SP-network operating on a block of four 32-bit words?

- **SHA-256**
- **CAST-128**
- **Serpent**
- **RC4**

Explanation
https://en.wikipedia.org/wiki/Serpent_(cipher)

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen.

Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. The cipher is a 32-round substitution–permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Serpent was designed so that all operations can be executed in parallel, using 32 bit slices. This maximizes parallelism, but also allows use of the extensive cryptanalysis work performed on DES.

Incorrect answers:

CAST-128 https://en.wikipedia.org/wiki/CAST-128

CAST-128 is a 12- or 16-round ***Feistel network*** with a 64-bit block size and a key size of between 40 and 128 bits

RC4 https://en.wikipedia.org/wiki/RC4

RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a ***stream cipher***.

SHA-256 https://en.wikipedia.org/wiki/SHA-2

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.

The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

Question 48:
Andrew, an evil hacker, research the website of the company which he wants to attack. During the research, he finds a web page and understands that the company's application is potentially vulnerable to Server-side Includes Injection. Which web-page file type did Andrew find while researching the site?

- **.cms**

- **.stm**
- **.html**
- **.rss**

Explanation

https://medium.com/@briskinfosec/server-side-includes-injection-4b2b624393c7

SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. They are similar to CGIs, except that SSIs are used to execute some actions before the current page is loaded or while the page is being visualized. In order to do so, the webserver analyzes SSI before supplying the page to the user.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

It is possible to check if the application is properly validating input fields data by inserting characters that are used in SSI directives, like:

< ! # = / . " - > and [a-zA-Z0-9]

Another way to discover if the application is vulnerable is to verify the presence of pages with extension .stm, .shtm and .shtml. However, the lack of these types of pages does not mean that the application is protected against SSI attacks.

In any case, the attack will be successful only if the webserver permits SSI execution without proper validation. This can lead to access and manipulation of file system and process under the permission of the webserver process owner.

Question 49:

Black-hat hacker Ivan attacked the SCADA system of the industrial water facility. During the exploration process, he discovered that outdated equipment was being used, the human-machine interface (HMI) was directly connected to the Internet and did not have any security tools or authentication mechanism. This allowed Ivan to control the system and influence all processes (including water pressure and temperature). What category does this vulnerability belong to?

- **Lack of Authorization/Authentication and Insecure Defaults.**
- **Code Injection.**
- **Memory Corruption.**
- **Credential Management.**

Explanation

https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities

Most SCADA / ICS equipment has a dedicated system for managing and monitoring industrial systems. Most people in the industry call this a human-machine interface or HMI. This system is essential for managing industrial systems, but it can also be an important vector for attackers. If an attacker could endanger the HMI, the attacker owns your industrial network. These systems have been compromised in at least two ways: protocol attacks and HMI attacks.

The major areas where SCADA software vulnerabilities occur as you can see in the graphic below are, respectively:

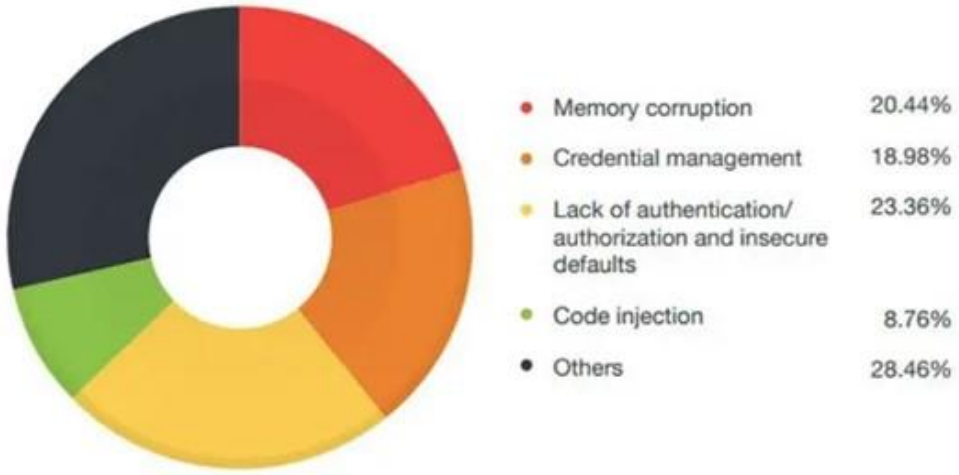
- Memory corruption.

- Credential management.

- Lack of authentication/authorization and insecure defaults.

- Code injection.

- A big chunk of other areas.



Memory corruption

The vulnerabilities in this category are code security issues that include out-of-bounds read/write vulnerabilities and heap- and stack-based buffer overflow.

Credential management

Includes all vulnerabilities from not protecting credentials enough and storing passwords in a recoverable format to the use of hard-coded passwords.

Lack of authentication/authorization and insecure defaults

The vulnerabilities in this category include transmission of confidential information in cleartext, insecure defaults, missing encryption, and insecure ActiveX controls used for scripting.

NOTE: The situation in the question relates to this vulnerability because the problem is not just in a simple password or in its insecure storage, but in the complete absence of the authentication mechanism itself.

Code injection

The vulnerabilities in this category include common code injections such as SQL, OS, command, and some domain-specific injections.

Question 50:
Identify what the following code is used for:

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

6. s.send(command+buffstring)
7. s.close()

- **Brute-force**
- **Heap spraying**
- **Buffer Overflow**
- **Buffer over-read**

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

This example shows a loop that fills up an array with “A”s in each iteration and sends them to the victim.

A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behavior, including memory access errors, incorrect results, and crashes.

Exploiting the behavior of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program, or the system as a whole, is well defined. By sending in data designed to cause a buffer overflow, it is possible to write into areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behavior that was not intended by the original programmer. Buffers are widespread in operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources. The famed Morris worm in 1988 used this as one of its attack techniques.

Incorrect answers:

Heap spraying https://en.wikipedia.org/wiki/Heap_spraying

Heap spraying is a technique used in exploits to facilitate arbitrary code execution. The part of the source code of an exploit that implements this technique is called a heap spray. In general, code that sprays the heap attempts to put a certain sequence of bytes at a predetermined location in the memory of a target process by having it allocate (large) blocks on the process's heap and fill the bytes in these blocks with the right values.

Buffer over-read https://en.wikipedia.org/wiki/Buffer_over-read

A buffer over-read is an anomaly where a program, while reading data from a buffer, overruns the buffer's boundary and reads (or tries to read) adjacent memory. This is a special case of violation of memory safety.

Buffer over-reads can be triggered, as in the Heartbleed bug, by maliciously crafted inputs that are designed to exploit a lack of bounds checking to read parts of memory not intended to be accessible. They may also be caused by programming errors alone. Buffer over-reads can result in erratic program behavior, including memory access errors, incorrect results, a

crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited to access privileged information.

Brute-force https://en.wikipedia.org/wiki/Brute-force_attack

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Question 51:
The attacker disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. His next step was to extract all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. Which of the following attacks was performed by the attacker?

- **Dictionary attack**
- **Rainbow table attack**
- **Internal monologue attack**
- **Phishing attack**

Explanation
https://github.com/eladshamir/Internal-Monologue

The Internal monologue attack allows NTLMv1 challenge-response hashes to be obtained from the victim's system, without injecting code in the memory or interacting with protected services such as the Local Security Authority Subsystem Service (LSASS). These hashes can then be cracked or subsequently used in a Pass-The-Hash (PTH) attack.

This technique allows a tester to obtain credentials from the system without touching the LSASS process. The attack takes advantage of the NetNTLMv1 challenge-response protocol. The NetNTLMv1 protocol is insecure due to the way it calculates the challenge-response allowing an attacker to retrieve the NTLM hash by easily cracking the response. Furthermore, retrieving the NTLM hash of a user is almost synonymous to retrieving the plaintext password of a user, since it can be used for a 'Pass the Hash' attack technique or can be cracked to obtain the plaintext password.

Although most modern systems are configured by default to avoid using NetNTLMv1, because the attacked is a local administrator of the system, a NetNTLM Downgrade attack can be performed to enable this weaker authentication scheme. This will disable preventive controls for NetNTLMv1. The attacker can then retrieve the non-network logon tokens from the running processes and impersonate the associated user.

Using the impersonated user privilege, the attacker can invoke a local procedure call to the NTLM authentication package called MSV1_0 to encrypt a known challenge using SSPI – secure single sign-on technology in Windows. This will generate a NetNTLMv1 response for that challenge using the impersonated user's NTLM hash as a key. Now, due to the weakness in the NetNTLMv1 challenge-response protocol, the tester can easily extract the NTLM hash by cracking this response and perform a 'Pass the Hash' attack.

Incorrect answers:

Dictionary attack https://en.wikipedia.org/wiki/Dictionary_attack

A dictionary attack is a form of brute force attack used for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

Rainbow table attack https://en.wikipedia.org/wiki/Rainbow_table

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

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

Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.

Question 52:
The attacker created a fraudulent email with a malicious attachment and sent it to employees of the target organization. The employee opened this email and clicked on the malicious attachment. Because of this, the malware was downloaded and injected into the software used in the victim's system occurred. Further, the malware propagated itself to other networked systems and finally damaging the industrial automation component. Which of the following attack techniques was used by the attacker?

- **Spear-phishing attack**
- **HMI-based attack**
- **Reconnaissance attack**
- **SMishing attack**

Explanation
Spear Phishing

Attackers send fake emails containing malicious links or attachments that seemingly originated from the victim's legitimate or well-known sources. When the victim clicks on the link or downloads the attachment, it injects malware, starts damaging the resources, and spreads itself to other systems. For example, an attacker sends a fraudulent email with a malicious attachment to a victim system that maintains the sales software of the operational plant. When the victim downloads the attachment, the malware is injected into the sales software, propagates itself to other networked systems, and finally damages industrial automation components.

Incorrect answers:

HMI-based attack

Human—Machine Interfaces (HMIIs) are often called Hacker—Machine Interfaces. Even with the advancement and automation of OT, human interaction and control over the operational process remain challenges due to the underlying vulnerabilities. The lack of global standards for developing HMI software without any defense-in-depth security measures leads to many security problems. Attackers exploit these vulnerabilities to perform various attacks such as memory corruption, code injection, privilege escalation, etc. on target OT systems.

SMishing attack

Smishing is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers. Smishing is implemented through text messages or SMS, giving the attack the name “SMiShing.”

Reconnaissance attack

Reconnaissance attacks are general knowledge gathering attacks. These attacks can happen in both logical and physical approaches. Whether the information is gathered via probing the network or through social engineering and physical surveillance, these attacks can be preventable as well. Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering and internet information queries.

Question 53:
Which of the following is a Kubernetes component that can assign nodes based on the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions?

- **Kube-scheduler**
- **Kube-controller-manager**
- **cloud-controller-manager**
- **Kube-apiserver**

Explanation
According to EC-Council courseware:

Kube-scheduler: Kube-scheduler is a master component that scans newly generated pods and allocates a node for them. It assigns the nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Kube-apiserver: The API server is an integral part of the Kubernetes control panel Module 19 Page 2834 that responds to all API requests. It serves as a front-end utility for the control panel and it is the only component that interacts with the etcd cluster and ensures data storage.

Kube-controller-manager: Kube-controller-manager is a master component that runs controllers. Controllers are generally individual processes (e.g., node controller, endpoint controller, replication controller, service account and token controller) but are combined into a single binary and run together in a single process to reduce complexity.

cloud-controller-manager: This is the master component used to run controllers that communicate with cloud providers. Cloud-controller-manager enables the Kubernetes code and cloud provider code to evolve separately.

Question 54:
Modern security mechanisms can stop various types of DDoS attacks, but if they only check incoming traffic and mostly ignore return traffic, attackers can bypass them under the disguise of a valid TCP session by carrying an SYN, multiple ACK, and one or more RST or FIN packets. What is the name of such an attack?

- **Spoofed session flood attack.**
- **UDP flood attack.**
- **Peer-to-peer attack.**
- **Ping-of-death attack.**

Explanation
https://ddos-guard.net/en/terminology/attack_type/fake-session-attack-spoofed-session-flood

The algorithm of this type of attacks comes down to TCP session emulation on networks with asymmetric routing: the attacker generates fake SYN-packets that are followed by a lot of ACK, and finally FIN/RST packets. All these packets resemble real TCP session traffic that is being sent from one host to another. Bearing in mind that today most networks have asymmetric traffic routing (in which incoming and outgoing packets are being sent via different routes), and modern network security tools are designed for the analysis of unidirectional traffic (and not for the analysis of return traffic), conditions for this type of attack are perfect. Thus, simulating TCP communication and bypassing security tools that analyze only the incoming traffic, the attacker can exhaust system resources and make the victim server inaccessible.

There are two types of such attacks:

1. The attack starts with sending several falsified SYN packets, followed by a number of ACK, and one or more FIN/RST packets;

2. Skipping SYN packets, the attack starts with sending multiple ACK, followed by one or more FIN/RST packets. Due to the relatively low speed used to send fake packets, it is more difficult to detect this type of attack than a regular flood, while achieving the same result: exhaustion of the victim server system resources.

Incorrect answers:

UDP flood attack https://en.wikipedia.org/wiki/UDP_flood_attack

Numerous fabricated UDP packets are fired at a server until it becomes unresponsive.

Peer-to-peer attack

https://en.wikipedia.org/wiki/Denial-of-service_attack#Peer-to-peer_attacks

A peer-to-peer DDoS attack is when an attacker exploits bugs in peer-to-peer servers to execute a DDoS attack.

Ping-of-death attack https://en.wikipedia.org/wiki/Ping_of_death

A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

Question 55:
Identify the security model by description:

In this security model, every user in the network maintains a ring of public keys. Also, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.

- **Web of trust**
- **Transport Layer Security**
- **Zero trust security model**
- **Secure Socket Layer**

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

A web of trust is a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). As with computer networks, there are many independent webs of trust, and any user (through their public key certificate) can be a part of, and a link between, multiple webs.

There are two keys pertaining to a person: a public key which is shared openly and a private key that is withheld by the owner. The owner's private key will decrypt any information encrypted with its public key. In the web of trust, ***each user has a ring with a group of people's public keys***.

Users encrypt their information with the recipient's public key, and only the recipient's private key will decrypt it. Each user then digitally signs the information with their private key, so when the recipient verifies it against the user's own public key, they can confirm that it is the user in question. Doing this will ensure that the information came from the specific user and has not been tampered with, and only the intended recipient can read the information (because only they know their private key).

Incorrect answers:

Transport Layer Security https://en.wikipedia.org/wiki/Transport_Layer_Security

Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible.

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. It runs in the application layer of the Internet and is itself composed of two layers: the TLS record and the TLS handshake protocols.

TLS is a proposed Internet Engineering Task Force (IETF) standard, first defined in 1999, and the current version is TLS 1.3 defined in August 2018. TLS builds on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator web browser.

Secure Sockets Layer

https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0

Secure Sockets Layer (SSL), is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

Zero trust security model https://en.wikipedia.org/wiki/Zero_trust_security_model

The zero trust security model (also, zero trust architecture, zero trust network architecture, ZTA, ZTA), sometimes known as perimeterless security, describes an approach to the design and implementation of IT systems. The main concept behind zero trust is “never trust, always verify,” which means that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified.

From late 2018, work undertaken in the U.S. by the NIST and National Cyber Security Center of Excellence (NCCoE) cyber security researchers led to A NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. The publication defines zero trust (ZT) as a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. A zero trust architecture (ZTA) is an enterprise's cyber security plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

An alternative but the consistent approach is taken by NCSC, in identifying the key principles behind zero trust architectures:

1. A single strong source of user identity

2. User authentication

3. Machine authentication

4. The additional context, such as policy compliance and device health

5. Authorization policies to access an application

6. Access control policies within an application

Question 56:
Scammers can query the DNS server to determine whether a specific DNS record is cached, thereby determining your organization’s browsing habits. This can disclose sensitive information such as financial institutions visited recently or other sensitive websites that a company might not want to be public knowledge of.

Which of the proposed attacks fits this description?

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

- **DNS cache poisoning**

Explanation
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-server-cache-snooping-attacks

DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.

This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.

This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.

DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. "lame requests").

Question 57:
Evil hacker Ivan knows that his target point and user are compatible with WPA2 and WPA 3 encryption mechanisms. He decided to install a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to connect. As soon as the connection is established, Ivan plans to use automated tools to crack WPA2-encrypted messages.

Which of the following attacks does Ivan want to perform?

- **Downgrade security attack**
- **Side-channel attack**
- **Cache-based attack**
- **Timing-based attack**

Explanation
https://www.welivesecurity.com/2019/04/11/wpa3-flaws-steal-wifi-passwords/

Downgrade Security Attacks

To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the attacker forces the user to follow the older encryption method, WPA2, to connect to the network. A downgrade security attack can be implemented in the following two ways.

- ***Exploiting backward compatibility:*** If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.

- Exploiting the Dragonfly handshake: In this method, the attacker masquerades as an authentic AP. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the attacker informs the user that it does not support the WPA3 method. Then, the attacker suggests the use of a weaker encryption mechanism

such as WPA2 for accessing the Internet. Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

Incorrect answers:

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

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g. through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University. Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher.

Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically considered side-channel attacks: see social engineering and rubber-hose cryptanalysis.

General classes of side-channel attack include:

Cache attack — attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.

Timing attack — attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.

Power-monitoring attack — attacks that make use of varying power consumption by the hardware during computation.

Electromagnetic attack — attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.

Acoustic cryptanalysis — attacks that exploit sound produced during a computation (rather like power analysis).

Differential fault analysis — in which secrets are discovered by introducing faults in a computation.

Data remanence — in which sensitive data are read after supposedly having been deleted. (i.e. Cold boot attack)

Software-initiated fault attacks — Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).

Optical - in which secrets and sensitive data can be read by visual recording using a high resolution camera, or other devices that have such capabilities (see examples below).

Question 58:
You are investigating to determine the reasons for compromising the computers of your company's employees. You will find out that the machines were infected through sites that employees often visit.

When an employee opens a site, there is a redirect from a web page, and malware downloads to the machine.

Which of the following attacks did the attacker perform on your company's employees?

- **Watering hole**
- **MarioNet**
- **Clickjacking**
- **DNS rebinding**

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

The watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. Eventually, some members of the targeted group will become infected. Hacks looking for specific information may only attack users coming from a specific IP address. This also makes the hacks harder to detect and research. The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.

Incorrect answers:

DNS rebinding https://en.wikipedia.org/wiki/DNS_rebinding

DNS rebinding is a method of manipulating resolution of domain names that is commonly used as a form of computer attack. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network. In theory, the same-origin policy prevents this from happening: client-side scripts are only allowed to access content on the same host that served the script. Comparing domain names is an essential part of enforcing this policy, so DNS rebinding circumvents this protection by abusing the Domain Name System (DNS).

This attack can be used to breach a private network by causing the victim's web browser to access computers at private IP addresses and return the results to the attacker. It can also be employed to use the victim machine for spamming, distributed denial-of-service attacks, or other malicious activities.

MarioNet https://hub.packtpub.com/marionet-a-browser-based-attack-that-allows-hackers-to-run-malicious-code-even-if-users-exit-a-web-page/

MarioNet allows attackers to place malicious code on high-traffic websites for a short period of time. This allows the attackers to gain a huge user base, remove the malicious code, but continue to control the infected browsers from another central server.

MarioNet allows hackers to assemble giant botnets from users' browsers. The researchers state that these bots can be used for in-browser crypto-mining (crypto jacking), DDoS attacks, malicious files hosting/sharing, distributed password cracking, creating proxy networks, advertising click-fraud, and traffic stats boosting.

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

Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages. Clickjacking is an instance of the confused deputy problem, wherein a computer is tricked into misusing its authority.

Question 59:
You want to prevent possible SQLi attacks on your site. To do this, you decide to use a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.

Which of the following practices are you going to adopt?

- **Enforce least privileges.**
- **Blacklist validation.**
- **Whitelist validation.**
- **Output encoding.**

Explanation
According to EC-council courseware:

Whitelist validation

Whitelist validation is a best practice whereby only the list of entities (i.e., data type, range, size, value, etc.) that have been approved for secured access is accepted. Whitelist validation can also be termed as positive validation or inclusion.

Blacklist Validation

Blacklist validation rejects all malicious inputs that have been disapproved for protected access. Blacklist validation can be challenging as every content and character of the attack should be interpreted, understood, and anticipated for future attacks as well. Blacklist validation can also be termed as negative validation or exclusion.

Output Encoding

Output encoding is a validation technique that can be used after input validation. This technique is used to encode the input to ensure that it is properly sanitized before passing it to the database.

Enforcing Least Privileges

Enforcing least privileges is a security best practice whereby the lowest level of privileges is assigned to every account accessing the database. It is recommended not to assign DBA level and administrator-level access rights to the application. In some critical situations, some applications may require elevated access rights; hence, proper groundwork should be done by the security professionals and they should also figure out the exact requirements of the application.

Question 60:
Which of the following services is running on port 21 by default?

- **Domain Name System**
- **Border Gateway Protocol**
- **Service Location Protocol**
- **File Transfer Protocol**

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

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

Port 21 - File Transfer Protocol (FTP)

Incorrect answers:

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

Port 179 - Border Gateway Protocol (BGP)

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

Port 427 - Service Location Protocol (SLP)

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

Port 53 - Domain Name System (DNS)

Question 61:
Which of the following is a Metasploit post-exploitation module that is used to escalate privileges on systems?

- **keylogrecorder**
- **getsystem**
- **getuid**
- **autoroute**

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

Metasploit has a Meterpreter script, **getsystem**, that will use a number of different techniques to attempt to gain SYSTEM level privileges on the remote system. There are also various other (local) exploits that can be used to also escalate privileges.

At the link above, you can see an example of using getsystem to escalate privileges.

Question 62:
Are you sure your network is perfectly protected and no evil hacker Ivan listens to all your traffic? What, ignorance is the greatest source of happiness. There is a powerful tool written in Go that will allow an attacker to carry out a Man in the middle (MITM) attack using, for example, ordinary arp spoofing. What kind of tool are we talking about?

- **DerpNSpoof**
- **Gobbler**
- **Wireshark**
- **BetterCAP**

Explanation
https://www.bettercap.org/

bettercap is a powerful, easily extensible and portable framework written in Go which aims to offer to security researchers, red teamers and reverse engineers an easy to use, all-in-one solution with all the features they might possibly need for performing reconnaissance and attacking WiFi networks, Bluetooth Low Energy devices, wireless HID devices and Ethernet networks.

One of the main feature is:

· ARP, DNS, NDP and DHCPv6 spoofers for MITM attacks on IPv4 and IPv6 based networks.

Incorrect answers:

Wireshark https://www.wireshark.org/

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

DerpNSpoof https://github.com/Trackbool/DerpNSpoof

Simple DNS Spoofing tool made in Python 3 with Scapy.

Gobbler http://gobbler.sourceforge.net/

Spoofed remote OS detection tool.

Question 63:
John, a black hat hacker, wants to find out if there are honeypots in the system that he will attack. For this purpose, he will use a time-based TCP fingerprinting method to validate the response to a computer and the response of a honeypot to a manual SYN request. Identify which of the following techniques will John use?

- **Detecting the presence of Snort_inline honeypots.**
- **Detecting the presence of UML Honeypot.**
- **Detecting the presence of Honeyd honeypots.**
- **Detecting the presence of Sebek-based honeypots.**

Explanation
Detecting the presence of Honeyd Honeypot*:*

Honeyd is a simulator honeypot engine that can create thousands of honeypots easily. The honeyd would respond to received SMTP requests with fake responses. An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods.

Incorrect answers:

Detecting the presence of User-Mode Linux (UML) Honeypot*:*

Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.

***Detecting the presence of Sebek-based Honeypots**:*

Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect.

***Detecting the presence of Snort_inline Honeypot**:*

Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker. When the snort_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.

Question 64:
During the pentest, Maria, the head of the blue team, discovered that the new online service has problems with the authentication mechanism. The old password can be reset by correctly answering the secret question, and the sending form does not have protection using a CAPTCHA, which allows a potential attacker to use a brute force attack. What is the name of such an attack in the Enumeration of Common Disadvantages (CWE)?

- **Insecure transmission of credentials.**
- **Verbose failure messages.**
- **User impersonation.**
- **Weak password recovery mechanism.**

Explanation
https://cwe.mitre.org/data/definitions/640.html

It is common for an application to have a mechanism that provides a means for a user to gain access to their account in the event they forget their password. Very often the password recovery mechanism is weak, which has the effect of making it more likely that it would be possible for a person other than the legitimate system user to gain access to that user's account. Weak password recovery schemes completely undermine a strong password authentication scheme.

This weakness may be that the security question is too easy to guess or find an answer to (e.g. because the question is too common, or the answers can be found using social media). Or there might be an implementation weakness in the password recovery mechanism code that may for instance trick the system into e-mailing the new password to an e-mail account other than that of the user. There might be no throttling done on the rate of password resets so that a legitimate user can be denied service by an attacker if an attacker tries to recover their password in a rapid succession. The system may send the original password to the user rather than generating a new temporary password. In summary, password recovery functionality, if not carefully designed and implemented can often become the system's weakest link that can be misused in a way that would allow an attacker to gain unauthorized access to the system.

Question 65:
Such techniques as, for example, password cracking or enumeration are much more efficient and faster if performed using a wordlist. Of course, there are a huge number of them in different directions on the Internet or already installed in your Kali or Parrot OS, but an attacker can create his wordlist specifically for the target he is attacking. This requires conducting intelligence and collecting information about the victim. Many tools allow you to automate this process.

Which of the following tools can scan a website and create a wordlist?

- **Psiphon**
- **Orbot**
- **CeWL**
- **Shadowsocks**

Explanation
https://tools.kali.org/password-attacks/cewl

CeWL is a ruby app which spiders a given url to a specified depth, optionally following external links, and returns a list of words which can then be used for password crackers such as John the Ripper.

Incorrect answers:

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

It is a free software Proxy server project to provide anonymity on the Internet for users of the Android operating system. It acts as an instance of the Tor network on such devices and allows traffic routing from a device's web browser, e-mail client, map program, etc., through the Tor network, providing anonymity for the user.

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

Its is a free and open-source encryption protocol project, widely used in China to circumvent Internet censorship.

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

It is a free and open-source Internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies (VPN, SSH, and HTTP Proxy). Psiphon is a centrally managed and geographically diverse network of thousands of proxy servers, using a performance-oriented, single- and multi-hop architecture.

Question 66:
Rajesh wants to make the Internet a little safer and uses his skills to scan the networks of various organizations and find vulnerabilities even without the owners' permission. He informs the company owner about the problems encountered, but if the company ignores him and does not fix the vulnerabilities, Rajesh publishes them publicly and forces the company to respond. What type of hacker is best suited for Rajesh?

- **Gray hat**
- **Cybercriminal**
- **White hat**
- **Black hat**

Explanation
https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner’s permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the problem. If the owner does not respond or comply, periodically, the hackers will post the newly found exploit online for the world to see.

These types of hackers are not inherently malicious with their intentions; they’re just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner before attacking the system.

Question 67:
Alexa, a college student, decided to go to a cafe. While waiting for her order, she decided to connect to a public Wi-Fi network without additional security tools such as a VPN. How can she verify that nobody is not performing an ARP spoofing attack on her laptop?

- **She should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.**
- **She can't identify such an attack and must use a VPN to protect her traffic.**
- **She should check her ARP table and see if there is one IP address with two different MAC addresses.**
- **She should use netstat to check for any suspicious connections with another IP address within the LAN.**

Explanation
https://www.comparitech.com/blog/information-security/arp-poisoning-spoofing-detect-prevent/

ARP poisoning can be detected in several different ways. You can use Windows' Command Prompt, an open-source packet analyzer such as Wireshark, or proprietary options such as XArp.

You can check the ARP attack in Command Prompt. First, open Command Prompt as an administrator. In the command line, enter:

arp -a

If the table contains ***two different IP addresses that share the same MAC address***, then you are probably undergoing an ARP poisoning attack.

You can read about other ways of detecting ARP spoofing here:

Wireshark: https://media.neliti.com/media/publications/263063-arp-spoofing-detection-via-wireshark-and-9a79ced5.pdf

XArp: http://www.xarp.net/#support

Question 68:
The attacker performs the attack using micro:bit and Btlejack, gradually executed different commands in the console. After executing this attack, he was able to read and export sensitive information shared between connected devices. Which of the following commands did the attacker use to hijack the connections?

- **btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s**
- **btlejack -f 0x9c68fd30 -t -m 0x1fffffffff**
- **btlejack -c any**
- **btlejack -s**

Explanation
https://github.com/virtualabs/btlejack

This question looks a bit strange and abstract. Nevertheless, you will meet a question on a similar topic on the exam.

To answer, you just need to look at the example of Btlejacking Using BtleJack presented in EC-Council's courseware.

Btlejacking is performed using the following steps.

1. Select target devices using the following command:

```
btlejack -d /dev/ttyACMO -d /dev/ttyACM2 -s
```

2. With the Btlejack tool, take a position within a radius of 5 m from the target devices.

3. Capture already established (live) as well as new Bluetooth low energy (BLE) connections using the following commands.

- Sniffing an existing connection:

```
btlejack -s
```

- Sniffing for new connections:

```
btlejack -c any
```

4. Once the connection is captured, perform a jamming operation using the following command:

```
btlejack -f 0x129f3244 -j
```

5. Start hijacking the connection using the following command:

```
btlejack -f 0x9c68fd30 -t -m 0xlfffffffff
```

6. The captured data can be converted into the pcap format using the following command:

```
btlejack -f 0xac56bc12 -x nordic -o capture.nordic.pcap
```

Question 69:
Experienced employees of the EC-Council monitor the market of security providers every day in search of the best solutions for your business. According to EC-Council experts, which vulnerability scanner combines comprehensive static and dynamic security checks to detect vulnerabilities such as XSS, File Inclusion, SQL injection, command execution, and more?

- **Saleae Logic Analyzer**
- **Syhunt Hybrid**
- **Cisco ASA**
- **AT&T USM Anywhere**

Explanation
https://www.syhunt.com/en/?n=Products.SyhuntHybrid

Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of-band attacks through Hybrid-Augmented Analysis (HAST).

With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux 64-bit.

Incorrect answers:

AT&T USM Anywhere https://cybersecurity.att.com/products/usm-anywhere

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on-premises, and in remote locations, helping you to detect threats virtually anywhere.

Saleae Logic Analyzer https://www.saleae.com/

It is a powerful logic analyzer that lets you record and display signals in your circuit, so you can debug it fast. From Arduino projects to spacecraft control systems, over 20,000 professionals and enthusiasts use Logic each month to debug and understand their electrical designs.

Cisco ASA https://en.wikipedia.org/wiki/Cisco_ASA

Cisco ASA (Adaptive Security Appliance)— is a series of hardware firewalls developed by Cisco Systems.

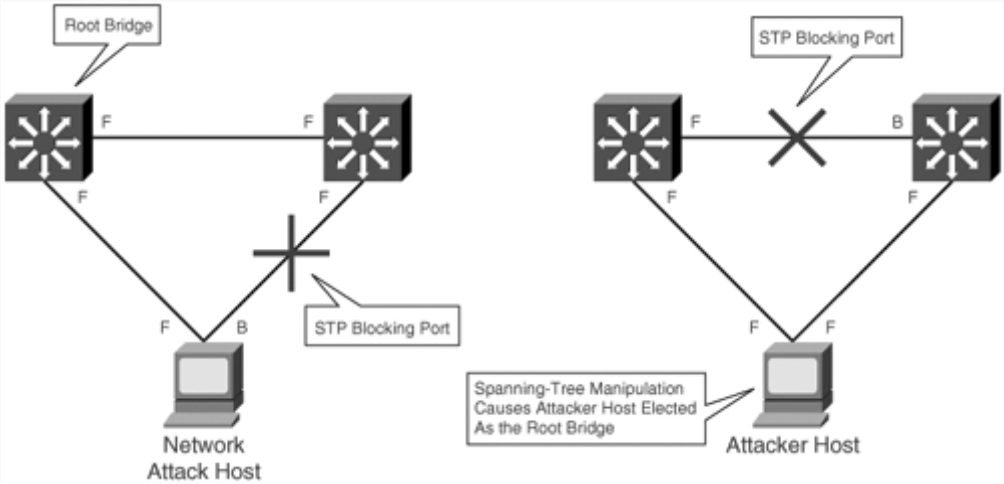
NOTE: I know I know. How will this "knowledge" help me in my work? It won't. This knowledge is required only for the exam.

Question 70:
Ivan, the black hat hacker, 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 target's network. What attack did Ivan perform?

- **VLAN hopping.**
- **ARP spoofing.**
- **DNS poisoning.**
- **STP attack.**

Explanation
https://howdoesinternetwork.com/2012/stp-attack

An STP attack involves an attacker spoofing 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. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes.



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 spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

VLAN hopping 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 71:
In which of the following Logging framework was a vulnerability discovered in December 2021 that could cause damage to millions of devices and Java applications?

- **Log4J**
- **Logback**
- **SLF4J**
- **Apache Commons Logging**

Explanation
https://logging.apache.org/log4j/2.x/security.html

https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

In December 2021, a vulnerability in the open-source Log4J logging service used by developers to monitor their Java applications first came to light, leaving enterprises scrambling to patch affected systems.

The Log4j exploit allows threat actors to take over compromised web-facing servers by feeding them a malicious text string. It exists within Log4j, an open-source Apache library for logging errors and events in Java-based applications. Third-party logging solutions like Log4j are a common way for software developers to log data within an application without building a custom solution.

The Log4J vulnerability is triggered by attackers inserting a JNDI lookup in a header field (likely to be logged) linking to a malicious server. After Log4j logs this string, the server is queried and gives directory information leading to the download and execution of a malicious java data class. This means cybercriminals can both extract private keys and, depending on the level of defenses in place, download and run malware directly on impacted servers.

Question 72:
You have been instructed to collect information about specific threats to the organization. You decide to collect the information from humans, social media, chat rooms, and events that resulted in cyberattacks. You also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks in this process. Thanks to this information, you were able to disclose potential risks and gain insight into attacker methodologies.

What is the type of threat intelligence collected by you?

- **Tactical threat intelligence.**
- **Strategic threat intelligence.**
- **Technical threat intelligence.**
- **Operational threat intelligence.**

Explanation
https://info-savvy.com/types-of-threat-intelligence/

Operational Threat Intelligence:

Operational threat intelligence provides info above specific threats against the organization. It provides contextual info above security events and incidents that help defenders disclose potential risks, offers bigger insight into offender methodologies, establishes past malicious activities, and performs investigations on malicious activity in a very more economical way. it's consumed by security managers or heads of incident response, network defenders, security forensics, and fraud detection groups.

It helps organizations understand the possible threat actors and their intention, capability, and opportunity to attack vulnerable IT assets, and also the impact of the attack if it's with success several cases, only government organizations will collect this type of intelligence, that also helps IR and forensic groups in deploying security assets with the aim of identifying and stopping future attacks, up the capability of detecting attacks at an early stage, and reducing its harm thereon assets.

Operational threat intelligence is mostly collected from sources like humans, social media and chat rooms, and additionally from real-world activities and events that lead to cyber-attacks. Operational threat intelligence is obtained by analyzing human behaviour, threat teams, and so on. This info helps in predicting future attacks and therefore enhancing incident response plans and mitigation ways as required. Operational threat intelligence is mostly within the kind of a report that contains known malicious activities, recommended courses of action, and warnings of emerging attacks.

Incorrect answers:

Strategic Threat Intelligence:

Strategic threat intelligence provides high-level information relating to cyber security posture, threats, details regarding the money impact of various cyber activities, attack trends, and the impacts of high-level business selections. This info is consumed by high-level executives and management of the organization like IT management and CISO. It helps the management in characteristic current cyber risks, unknown future risks, threat teams, and attribution of breaches. The intelligence obtained provides a risk primarily based read that primarily focuses on high-level ideas of risks and their chance.

It primarily focuses on long-term problems and provides a period of time alerts of threats on an organization's vital assets like IT infrastructure, employees, customers, and applications.

This type of threat intelligence is employed by the management to require strategic business selections and to investigate the results of such decisions. supported the analysis, the management will assign comfortable budgets and employees to guard vital IT assets and business processes.

Tactical Threat Intelligence:

Tactical threat intelligence plays a serious role in protecting the resources of the organization. It provides info related to TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cyber security professionals such as IT service managers, security operations managers, network operations center {NOC) employees, administrators, and architects.

It helps the cyber security professionals understand however the adversaries area unit expected to perform the attack on the set-up; identify the knowledge leakage from the organization, and the technical capabilities and goals of the attackers alongside the attack vectors. Using tactical threat intelligence security personnel develop detection and mitigation ways beforehand by change security merchandise with known indicators, patching vulnerable systems, etc.

The collection sources for tactical threat intelligence embrace campaign reports, malware, incident reports, attack group reports, human intelligence, etc. This intelligence is mostly obtained by reading white/technical papers, communicating with different organizations, or getting intelligence from third parties. It includes extremely technical info like malware, campaigns, techniques, and tools within the form of forensic reports.

Technical Threat Intelligence:

Technical threat intelligence provides information above an attacker's resources that are used to perform the attack; this includes command and control channels, tools, etc. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific loC. It provides rapid distribution and response to threats.

For example, a malware used to perform an attack is tactical threat intelligence, where as the details related to the specific implementation of the malware come under technical threat intelligence. Other examples of technical threat intelligence include specific IP addresses and domains used by malicious endpoints, phishing email headers, the hash checksum of malware, etc. Technical threat intelligence is consumed by SOC staff and IR teams.

The indicators of technical threat intelligence are collected from active campaigns, attacks that are performed on other organizations, or data feeds provided by external third parties. These inculcators are generally collected as part of investigations on attacks performed on various organizations. This information helps security professionals add the identified indicators to the defensive systems such as 105/IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify the attacks at an early stage. It also helps them identify malicious traffic and suspected IP addresses used to spread malware and spam mails. This intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Question 73:
Identify the technology according to the description:

It's an open-source technology that can help in developing, packaging, and running applications. Also, the technology provides PaaS through OS-level virtualization, delivers

containerized software packages, and promotes fast software delivery. This technology can isolate applications from the underlying infrastructure and stimulating communication via well-defined channels.

- **Serverless computing**
- **Paravirtualization**
- **Docker**
- **Virtual machine**

Explanation
https://en.wikipedia.org/wiki/Docker_(software)

Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels. Because all of the containers share the services of a single operating system kernel, they use fewer resources than virtual machines.

Incorrect answers:

Virtual machine https://en.wikipedia.org/wiki/Virtual_machine

A virtual machine (VM) is the virtualization/emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

Virtual machines differ and are organized by their function, shown here:

- System virtual machines (also termed full virtualization VMs) provide a substitute for a real machine. They provide functionality needed to execute entire operating systems. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Modern hypervisors use hardware-assisted virtualization, virtualization-specific hardware, primarily from the host CPUs.

- Process virtual machines are designed to execute computer programs in a platform-independent environment.

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

Paravirtualization or para-virtualization is a virtualization technique that presents a software interface to the virtual machines which is similar, yet not identical to the underlying hardware–software interface.

The intent of the modified interface is to reduce the portion of the guest's execution time spent performing operations which are substantially more difficult to run in a virtual environment compared to a non-virtualized environment. The paravirtualization provides specially defined 'hooks' to allow the guest(s) and host to request and acknowledge these tasks, which would otherwise be executed in the virtual domain (where execution performance is worse). A successful paravirtualized platform may allow the virtual machine monitor (VMM) to be simpler (by relocating execution of critical tasks from the virtual domain to the host domain), and/or reduce the overall performance degradation of machine execution inside the virtual guest.

Serverless computing https://en.wikipedia.org/wiki/Serverless_computing

Serverless computing is a cloud computing execution model in which the cloud provider allocates machine resources on demand, taking care of the servers on behalf of their customers. Serverless computing does not hold resources in volatile memory; computing is rather done in short bursts with the results persisted to storage. When an app is not in use, there are no computing resources allocated to the app. Pricing is based on the actual amount of resources consumed by an application. It can be a form of utility computing. "Serverless" is a misnomer in the sense that servers are still used by cloud service providers to execute code for developers. However, developers of serverless applications are not concerned with capacity planning, configuration, management, maintenance, fault tolerance, or scaling of containers, VMs, or physical servers.

Question 74:
Alex received an order to conduct a pentest and scan a specific server. When receiving the technical task, he noticed the point: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses." Which of the following Nmap flags will allow Alex to fulfill this requirement?

- **-D**
- **-S**
- **-f**
- **-A**

Explanation
https://linux.die.net/man/1/nmap

-D decoy1[,decoy2][,ME][,...] (Cloak a scan with decoys).

Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus their IDS might report 5-10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys. While this can be defeated through router path tracing, response-dropping, and other active mechanisms, it is generally an effective technique for hiding your IP address. Separate each decoy host with commas, and you can optionally use ME. as one of the decoys to represent the position for your real IP address. If you put ME in the sixth position or later, some common port scan detectors (such as Solar Designer's. excellent Scanlogd). are unlikely to show your IP address at all. If you don't use ME, Nmap will put you in a random position. You can also use RND. to generate a random, non-reserved IP address, or RND:number to generate number addresses.

Incorrect answers:

-f (fragment packets); --mtu (using the specified MTU).

The -f option causes the requested scan (including ping scans) to use tiny fragmented IP packets. The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing. Be careful with this! Some programs have trouble handling these tiny packets. The old-school sniffer named Sniffit segmentation faulted immediately upon receiving the first fragment. Specify this option once, and Nmap splits the packets into eight bytes or less after the IP header. So a 20-byte TCP header would be split into three packets. Two with eight bytes of the TCP header, and one with the final four. Of course each fragment also has an IP header. Specify -f again to use 16 bytes per fragment (reducing the number of fragments).

-S IP_Address (Spoof source address).

In some circumstances, Nmap may not be able to determine your source address (Nmap will tell you if this is the case). In this situation, use -S with the IP address of the interface you wish to send packets through.

-A (Aggressive scan options).

This option enables additional advanced and aggressive options. I haven't decided exactly which it stands for yet. Presently this enables OS detection (**-O**), version scanning (**-sV**), script scanning (**-sC**) and traceroute (**--traceroute**).. More features may be added in the future. The point is to enable a comprehensive set of scan options without people having to remember a large set of flags. However, because script scanning with the default set is considered intrusive, you should not use **-A** against target networks without permission. This option only enables features, and not timing options (such as **-T4**) or verbosity options (**-v**) that you might want as well.

Question 75:
Assume you used Nmap, and after applying a command, you got the following output:

1. Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
2. Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
3. Not shown: 932 filtered ports, 56 closed ports
4.
5. PORT STATE SERVICE -
6. 21/Rep open ftp
7. 22/tcp open ssh
8. 25/tcp open smtp
9. 53/tcp open domain
10. 80/tcp open http
11. 110/tcp open pop3
12. 143/tcp open imap
13. 443/tcp open https
14. 465/tcp open smtps
15. 587/tcp open submission
16. 993/tcp open imaps
17. 995/tcp open pop3s
18. Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds

Which of the following command-line parameter could you use to determine the service protocol, the application name, the version number, hostname, device type?

- **-sS**
- **-sV**
- **-sT**
- **-sY**

Explanation
https://nmap.org/book/man-version-detection.html

Point Nmap at a remote machine and it might tell you that ports 25/tcp, 80/tcp, and 53/udp are open. Using its nmap-services database of about 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate—the vast majority of daemons listening on TCP port 25 are, in fact, mail servers. However, you should not bet your security on this! People can and do run services on strange ports.

Even if Nmap is right, and the hypothetical server above is running SMTP, HTTP, and DNS servers, that is not a lot of information. When doing vulnerability assessments (or even simple network inventories) of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps

dramatically in determining which exploits a server is vulnerable to. Version detection helps you obtain this information.

After TCP and/or UDP ports are discovered using one of the other scan methods, version detection interrogates those ports to determine more about what is actually running. The nmap-service-probes database contains probes for querying various services and match expressions to recognize and parse responses. Nmap tries to determine the service protocol (e.g. FTP, SSH, Telnet, HTTP), the application name (e.g. ISC BIND, Apache httpd, Solaris telnetd), the version number, hostname, device type (e.g. printer, router), the OS family (e.g. Windows, Linux). When possible, Nmap also gets the Common Platform Enumeration (CPE) representation of this information. Sometimes miscellaneous details like whether an X server is open to connections, the SSH protocol version, or the KaZaA user name, are available. Of course, most services don't provide all of this information. If Nmap was compiled with OpenSSL support, it will connect to SSL servers to deduce the service listening behind that encryption layer. Some UDP ports are left in the open|filtered state after a UDP port scan is unable to determine whether the port is open or filtered. Version detection will try to elicit a response from these ports (just as it does with open ports), and change the state to open if it succeeds. open|filtered TCP ports are treated the same way. Note that the Nmap -A option enables version detection among other things.

When RPC services are discovered, the Nmap RPC grinder is automatically used to determine the RPC program and version numbers. It takes all the TCP/UDP ports detected as RPC and floods them with SunRPC program NULL commands in an attempt to determine whether they are RPC ports, and if so, what program and version number they serve up. Thus you can effectively obtain the same info as **rpcinfo -p** even if the target's portmapper is behind a firewall (or protected by TCP wrappers). Decoys do not currently work with RPC scan.

When Nmap receives responses from a service but cannot match them to its database, it prints out a special fingerprint and a URL for you to submit it to if you know for sure what is running on the port. Please take a couple minutes to make the submission so that your find can benefit everyone. Thanks to these submissions, Nmap has about 6,500 pattern matches for more than 650 protocols such as SMTP, FTP, HTTP, etc.

-sV (Version detection)

Enables version detection, as discussed above. Alternatively, you can use -A, which enables version detection among other things.

Incorrect answers:

-sS (TCP SYN scan)

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan 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 the open, closed, and filtered states.

-sT (TCP connect scan)

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. 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. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

-sY (SCTP INIT scan)

SCTP is a relatively new alternative to the TCP and UDP protocols, combining most characteristics of TCP and UDP, and also adding new features like multi-homing and multi-streaming. It is mostly being used for SS7/SIGTRAN related services but has the potential to be used for other applications as well. SCTP INIT scan is the SCTP equivalent of a TCP SYN scan. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. Like SYN scan, INIT scan is relatively unobtrusive and stealthy, since it never completes SCTP associations. It also allows clear, reliable differentiation between the open, closed, and filtered states.

Question 76:
The attacker gained credentials of an organization's internal server system and often logged in outside work hours. The organization commissioned the cybersecurity department to analyze the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response process, in which the cybersecurity department has determined these issues?

- **Eradication.**
- **Preparation.**
- **Incident triage.**
- **Incident recording and assignment.**

Explanation
According to the EC-Council's training materials:

Preparation

The preparation phase includes performing an audit of resources and assets to

determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, gathering required tools, and training the employees to secure their systems and accounts.

Incident recording and assignment

In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

Incident triage

In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and any vulnerabilities it exploited.

Eradication

In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

Question 77:
You have been instructed to organize the possibility of working remotely for employees. Their remote connections could be exposed to session hijacking during the work, and you want to prevent this possibility. You decide to use the technology that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. Which of the following technologies will you use?

- **VPN**
- **Split tunneling**
- **DMZ**
- **Bastion host**

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

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. The benefits of a VPN include increases in functionality, security, and management of the private network. It provides access to resources inaccessible on the public network and is typically used for telecommuting workers. Encryption is common, although not an inherent part of a VPN connection. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunnelling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Incorrect answers:

Split tunneling https://en.wikipedia.org/wiki/Split_tunneling

Split tunneling is a computer networking concept which allows a user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections. This connection state is usually facilitated through the simultaneous use of a Local Area Network (LAN) Network Interface Card (NIC), radio NIC, Wireless Local Area Network (WLAN) NIC, and VPN client software application without the benefit of access control.

DMZ https://en.wikipedia.org/wiki/DMZ_(computing)

DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

Bastion host https://en.wikipedia.org/wiki/Bastion_host

A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application or process, for example, a proxy server or load balancer, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of a firewall or inside of a demilitarized zone (DMZ) and usually involves access from untrusted networks or computers. These computers are also equipped with special networking interfaces to withstand high-bandwidth attacks through the internet.

Question 78:
`sqlmap.py -u "http://10.10.37.12/?p=1&forumaction=search" --dbs`

Which of the following does this command do?

- **Creating backdoors using SQL injection.**
- **Enumerating the databases in the DBMS for the URL.**
- **Retrieving SQL statements being executed on the database.**
- **Searching database statements at the IP address given.**

Explanation
http://manpages.org/sqlmap

-u URL, **--url**=*,URL/*

Target URL (e.g. "http://www.site.com/vuln.php?id=1")

--dbs

Enumerate DBMS databases

Question 79:
The company hired a cybersecurity specialist to conduct an audit of their mobile application.

On the first day of work, the specialist suggested starting with the fact that he would extract the source code of a mobile application and disassemble the application to analyze its design flaws. He is sure that using this technique, he can fix bugs in the application, discover underlying vulnerabilities, and improve defence strategies against attacks.

Which of the following techniques will the specialist use?

- **Jailbreaking.**
- **Reverse engineering.**
- **Rooting.**
- **Application sandboxing.**

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

https://securitytoday.com/articles/2019/02/26/reverse-engineering-is-one-of-your-best-weapons-in-the-fight-against-cyberattacks.aspx

Reverse engineering (also known as backwards engineering or back engineering) is a process or method through the application of which one attempts to understand through deductive reasoning how a device, process, system, or piece of software accomplishes a task with very little (if any) insight into exactly how it does so.

Security experts can apply reverse engineering themselves to understand how hard it is to hack certain software. If it turns out to be a breeze, experts can provide recommendations on ways to complicate matters for a potential hacker. This technique can be especially useful for security software developers who work in a wide range of data formats and protocols, conduct lots of research for client issues, and ensure code's compatibility with third-party software.

Incorrect answers:

Application sandboxing https://en.wikipedia.org/wiki/Sandbox_(computer_security)

A sandbox (including application sandboxing) is a security mechanism for separating running programs, usually in an effort to mitigate system failures and/or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system. A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as storage and memory scratch space. Network access, the ability to inspect the host system, or read from input devices are usually disallowed or heavily restricted.

Jailbreaking https://en.wikipedia.org/wiki/Jailbreaking_of_Apple_devices

Jailbreaking refers to privilege escalation on an Apple device to remove software restrictions imposed by Apple on iOS operating systems. Typically it is done through a series of kernel patches. A jailbroken device permits root access within the operating system and provides the opportunity to install software not available through the iOS App Store. Different devices and versions are exploited with a variety of tools. Apple views jailbreaking as a violation of the end-user license agreement, and strongly cautions device owners from attempting to achieve root access through the exploitation of vulnerabilities.

Rooting https://en.wikipedia.org/wiki/Rooting_(Android)

Rooting is the process of allowing users of the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems. As Android is based on a modified version of the Linux kernel, rooting an Android device gives similar access to administrative (superuser) permissions as on Linux or any other Unix-like operating system such as FreeBSD or macOS.

Question 80:
The attacker wants to draw a map of the target organization's network infrastructure to know about the actual environment they will hack. Which of the following will allow him to do this?

- **Vulnerability analysis**
- **Malware analysis**
- **Network enumeration**
- **Scanning networks**

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

https://w4rri0r.com/hacking-tools-windows-os-x-linux-android-solaris-unixware/network-mapping.html

It would be much more logical to use the phrase "Network mapper," but you can meet a question on this topic with exactly this wording on the exam.

The network map provides a topology view of your network to help you visualize network partitions, dependencies, and bottlenecks.

Network mapping is the process of visualizing all the devices on network, how they're connected, and how the overall network is structured.

There are two main levels of maps to consider: physical and logical. While open-source network mapping tools can create a physical network map, they may not offer automated scanning to ensure the map is always up to date.

There are three levels of maps to consider—***physical, logical, and functional.***

A physical network map diagrams all the actual components of your network, including cords, plugs, racks, ports, servers, cables, and more. A physical network map gives you a visual representation of all the material elements of your network and the connections between them.

A logical map is more abstract than the physical network map. It shows the type of network topology (bus, ring, etc.), and how the data flows between the physical objects in your network. This includes IP addresses, firewalls, routers, subnets and subnet masks, traffic flow, voice gateways, and other segments of the network.

To note: Since logical and physical network maps depict the same network environment from two different perspectives, it's best to use both types to get a more comprehensive look at your network.

A functional network map shows you how application traffic flows through the network physically. These types of network maps are only as useful as they are accurate, which means you need an appropriate and high-quality tool.

Incorrect answers:

Vulnerability Analysis

A vulnerability analysis is a review that focuses on security-relevant issues that either moderately or severely impact the security of the product or system.

Malware analysis https://en.wikipedia.org/wiki/Malware_analysis

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor. Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies. Malware may include software that gathers user information without permission.

Network enumeration https://en.wikipedia.org/wiki/Network_enumeration

Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It should not be confused with network mapping, which only retrieves information about which servers are connected to a specific network and what operating system runs on them. Network enumeration is the discovery of hosts or devices on a network. Network enumeration tends to use overt discovery protocols such as ICMP and SNMP to gather information. It may also scan various ports on remote hosts for looking for well known services in an attempt to further identify the

function of a remote host. The next stage of enumeration is to fingerprint the operating system of the remote host.

Question 81:
Which of the following is a type of malware that spreads from one system to another or from one network to another and causes similar types of damage as viruses to do to the infected system?

- **Worm**
- **Rootkit**
- **Adware**
- **Trojan**

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

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue. Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Incorrect answers:

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

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a compound of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it after having obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

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

Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process. The software may generate two types of revenue: one is for the display of the advertisement and another on a "pay-per-click" basis, if the user clicks on the advertisement. Some advertisements also act as spyware, collecting and reporting data about the user, to be sold or used for targeted advertising or user profiling. The software may implement advertisements in a variety of ways, including a static box display, a banner display, full

screen, a video, pop-up ad or in some other form. All forms of advertising carry health, ethical, privacy and security risks for users.

Trojan https://en.wikipedia.org/wiki/Trojan_horse_(computing)

A Trojan horse (or simply trojan) is any malware that misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Ransomware attacks are often carried out using a trojan.

Question 82:

```
<!DOCTYPE checksomething [<!ENTITY xxx SYSTEM "file:///etc/passwd">]>
```

In which of the following attacks is the line above injected?

- **XXS**
- **IDOR**
- **XXE**
- **SQLi**

Explanation

https://portswigger.net/web-security/xxe

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem and interact with any back-end or external systems that the application can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

Incorrect answers:

SQLi https://en.wikipedia.org/wiki/SQL_injection

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

XXS https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability that can be found in some 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.

IDOR https://portswigger.net/web-security/access-control/idor

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. However, it is just one example of many access control implementation mistakes that can lead to access controls being circumvented. IDOR vulnerabilities are most commonly associated with horizontal privilege escalation, but they can also arise in relation to vertical privilege escalation

Question 83:
At which of the following steps of the Cyber Kill Chain is the creation of a malware weapon, for example, such as a malicious file disguised as a financial spreadsheet?

- **Reconnaissance**
- **Exploitation**
- **Delivery**
- **Weaponization**

Explanation
https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/

The Cyber Kill Chain offers a comprehensive framework as a part of the Intelligence Driven Defense model.

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 in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as zero-day exploits) or it can focus on a combination of different vulnerabilities.

3. Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different methods like 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 84:
Have you spent a lot of time and money on creating photo materials for your business? You probably don't want anyone else to use them. But you don't need to hire a cool hacker to solve this problem. There is a reasonably simple method using search engines to search for photographs, profile pictures, and memes.

What method are we talking about?

- **Google advanced search**
- **Google dorking**
- **Reverse image search**
- **Metasearch engines**

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

Reverse image search is a ***content-based image retrieval (CBIR)*** query technique that involves providing the CBIR system with a sample image that it will then base its search upon; in terms of information retrieval, the sample image is what formulates a search query. In particular, reverse image search is characterized by a lack of search terms. This effectively removes the need for a user to guess at keywords or terms that may or may not return a correct result. Reverse image search also allows users to discover content that is related to a specific sample image, popularity of an image, and discover manipulated versions and derivative works.

Incorrect answers:

Google advanced search https://www.google.com/advanced_search

Google Advanced Search is a more detailed method of finding information on Google. It uses a variety of Google search operators that consists of special characters and commands – also known as “advanced operators” – that goes beyond a normal Google search.

Metasearch engines https://en.wikipedia.org/wiki/Metasearch_engine

A metasearch engine (or search aggregator) is an online information retrieval tool that uses the data of a web search engine to produce its own results. Metasearch engines take input from a user and immediately query search engines for results. Sufficient data is gathered, ranked, and presented to the users.

Google dorking https://en.wikipedia.org/wiki/Google_hacking

Google hacking, also named Google dorking, 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.

Question 85:
Black-hat hacker Ivan attacked a large DNS server. By poisoning the cache, he was able to redirect the online store's traffic to a phishing site. Users did not notice the problem and believed that they were on the store's actual website, so they entered the data of their accounts and even bank cards. Before the security system had time to react, Ivan collected a large amount of critical user data.

Which option is best suited to describe this attack?

- **SPIT attack**
- **Spear-phishing**
- **Pharming**
- **Phishing**

Explanation
https://csrc.nist.gov/glossary/term/pharming

An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name System), causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software, or contribute to a fraudulent act.

There are a couple of different forms of pharming. In one form, code sent in an email modifies local host files on a PC. The host files convert Uniform Resource Locators (URLs) into the IP address that the computer uses to access websites. A computer with a compromised host file will go to the fake site even if a user types in the correct web address or clicks on an affected bookmark entry.

Another pharming tactic is DNS poisoning. The DNS table in a server is modified, so someone who thinks they are accessing legitimate websites is directed toward fraudulent ones. In this method of pharming, individual PC host files don't need to be corrupted. Instead, the problem occurs in the DNS server, which handles millions of internet users' URL requests. Victims then end up at a bogus site without any visible indicator of a discrepancy.

Incorrect answers:

Spear-phishing https://en.wikipedia.org/wiki/Phishing#Spear_phishing

Spear phishing involves an attacker directly targeting a specific organization or person with tailored phishing emails. This is essentially the creation and sending of emails to a particular person to make the person think the email is legitimate. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success of the attack.

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

Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

SPIT attack https://en.wikipedia.org/wiki/VoIP_spam

VoIP spam or SPIT (spam over Internet telephony) is unsolicited, automatically dialed telephone calls, typically using voice over Internet Protocol (VoIP) technology. VoIP systems, like e-mail and other Internet applications, are susceptible to abuse by malicious

parties who initiate unsolicited and unwanted communications, such as telemarketers and prank callers.

Question 86:
Lisandro was hired to steal critical business documents of a competitor company. Using a vulnerability in over-the-air programming (OTA programming) on Android smartphones, he sends messages to company employees on behalf of the network operator, asking them to enter a PIN code and accept new updates for the phone. After the employee enters the PIN code, Lisandro gets the opportunity to intercept all Internet traffic from the phone. What type of attack did Lisandro use?

- **Bypass SSL pinning.**
- **Advanced SMS phishing.**
- **Tap 'n ghost attack.**
- **Social engineering.**

Explanation
https://en.wikipedia.org/wiki/Over-the-air_programming

An over-the-air (OTA) update is the wireless delivery of new software, firmware, or other data to mobile devices. This technology has grown more prominent with the growth of mobile devices and applications. Mobile operators and telecommunication third parties can send OTA updates through SMS to configure data updates in SIM cards, distribute system updates, or access services, such as wireless access protocol (WAP) or multimedia messaging service (MMS). OTA updates also enable mobile operators to activate user subscriptions. OEMs can use OTA updates to fix bugs through firmware and change the user interface. The proliferation of IoT has led manufacturers to use OTA updates for autonomous vehicles, smart home speakers, and other IoT devices.

The following link presents an investigation by Check Point Researchers:

Advanced SMS Phishing Attacks Against Modern Android-based Smartphones

A security flaw in Samsung, LG, Sony, Huawei and other Android smartphones has been discovered that leaves users vulnerable to advanced SMS phishing attacks, Check Point Research -- the threat intelligence arm of cybersecurity firm Check Point Software Technologies Ltd. said on Thursday.

Researchers at the cybersecurity firm said certain Samsung phones are the most vulnerable to this form of phishing attack because they do not have an authenticity check for senders of Open Mobile Alliance Client Provisioning (OMA CP) messages.

The affected Android phones use OTA provisioning, through which cellular network operators can deploy network-specific settings to a new phone joining their network.

However, researchers at Check Point found that the industry standard for OTA provisioning -- the OMA CP, includes limited authentication methods and remote agents can exploit this to pose as network operators and send deceptive OMA CP messages to users.

The message tricks users into accepting malicious settings that route their Internet traffic through a proxy server owned by the hacker.

NOTE: For the exam, it is enough just to know about this type of attack, but I advise you to read the full investigation - it is very interesting. This vulnerability affected a lot of Android phones, but it was quickly discovered and vendors released patches to fix it. Nevertheless, this vulnerability gave rise to a new level of smishing attacks - Advanced SMS Phishing.

Question 87:
In which of the following cloud service models do you take full responsibility for the maintenance of the cloud-based resources?

- **PaaS**
- **IaaS**
- **SaaS**
- **BaaS**

Explanation
https://www.intel.ru/content/www/ru/ru/cloud-computing/as-a-service.html

IaaS (Infrastructure as a service)

IaaS is on-demand access to cloud-hosted computing infrastructure - servers, storage capacity, and networking resources - that customers can provision, configure and use in much the same way as they use on-premises hardware. The difference is that the cloud service provider hosts manages and maintains the hardware and computing resources in its own data centers. IaaS customers use the hardware via an internet connection and pay for that use on a subscription or pay-as-you-go basis.

PaaS (Platform as a service)

PaaS provides a cloud-based platform for developing, running, managing applications. The cloud services provider hosts, manages and maintains all the hardware and software included in the platform - servers (for development, testing and deployment), operating system (OS) software, storage, networking, databases, middleware, runtimes, frameworks, development tools - as well as related services for security, operating system and software upgrades, backups and more.

SaaS (Software as a service)

SaaS is cloud-hosted, ready-to-use application software. Users pay a monthly or annual fee to use a complete application from within a web browser, desktop client, or mobile app. The application and all of the infrastructure required to deliver it - servers, storage, networking, middleware, application software, data storage - are hosted and managed by the SaaS vendor.

BaaS (Backend as a Service)

BaaS takes care of all the backend services of an application, and the developers can focus only on writing and maintaining the frontend side of the application. It provides backend services like database management, user authentication, cloud storage, hosting on the cloud, push notifications, etc.

Question 88:
Passwords are rarely stored in plain text, most often, one-way conversion (hashing) is performed to protect them from unauthorized access. However, there are some attacks and tools to crack the hash. Look at the following tools and select the one that can NOT be used for this.

- **Hashcat**
- **Netcat**
- **Ophcrack**
- **John the Ripper**

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

Most systems don't store passwords on them. Instead they store hashes of passwords and when authentication takes place, the password is hashes and if the hashes match authentication is successful. Different systems store password hashes in different ways depending on the encryption used.

Password hash cracking usually consists of taking a wordlist, hashing each word and comparing it against the hash you're trying to crack. This is a variation of a dictionary attack because wordlists often are composed of not just dictionary words but also passwords from public password dumps. This type of cracking becomes difficult when hashes are salted).

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

Netcat is a utility capable of establishing a TCP or UDP connection between two computers, meaning it can write and read through an open port. With the help of the program, files can be transferred and commands can be executed in some instances.

Incorrect answers:

Hashcat https://hashcat.net/

Hackers use Hashcat to automate attacks against passwords and other shared secrets. It gives the user the ability to brute-force credential stores using known hashes, to conduct dictionary attacks and rainbow tables, and to reverse engineer readable information on user behavior into hashed-password combination attacks.

John the Ripper https://www.openwall.com/john/

John the Ripper is an offline password cracker. In other words, it tries to find passwords from captured files without having to interact with the target. By doing this, it does not generate suspicious traffic since the process is generally performed locally, on the attacker's machine.

Although it's primarily used to crack password hashes, John can also be used to crack protected archive files, encrypted private keys, and many more.

Ophcrack https://ophcrack.sourceforge.io/

Ophcrack is a password cracker based on rainbow tables, a method that makes it possible to speed up the cracking process by using the result of calculations done in advance and stored rainbow tables.

Question 89:
Ivan, a black hacker, wants to attack the target company. He thought about the fact that vulnerable IoT devices could be used in the company. To check this, he decides to use the tool, scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials. Which of the following tools will Ivan use?

- **IoTSeeker**
- **Cloud IoT Core**
- **Bullguard IoT**
- **Azure IoT Central**

Explanation
IoTSeeker

https://github.com/rapid7/IoTSeeker

This scanner will scan a network for specific types of IoT devices to detect if they are using the default, factory-set credentials. The recent Internet outage has been attributed to use the IoT devices (CCTV Cameras, DVRs and others) with default credentials. It's the intention of this tool to help organizations scan their networks to detect these types of IoT devices and to identify whether credentials have been changed or if the device is still using the factory setting. Note that Mirai malware, suspected to have been used to launch the massive internet outage on Oct 21, 2016, mainly focuses on telnet services. IoTSeeker focuses on HTTP/HTTPS services.

Incorrect answers:

Bullguard IoT https://iotscanner.azurewebsites.net/

Bullguard‘s solution checks if your internet-connected devices at home are public on Shodan, the world’s first search engine for Internet-connected devices. If the result is positive, this means that the public, including hackers, can access them.

Knowing if your devices are public on Shodan represents a warning sign, allowing you to take further measures to improve your devices’ security level.

Azure IoT Central https://azure.microsoft.com/en-us/services/iot-central/#overview

Azure IoT Central is an IoT application platform that reduces the burden and cost of developing, managing, and maintaining enterprise-grade IoT solutions. Choosing to build with IoT Central gives you the opportunity to focus time, money, and energy on transforming your business with IoT data, rather than just maintaining and updating a complex and continually evolving IoT infrastructure.

Cloud IoT Core https://developers.google.com/iot

IoT Core is a fully managed service that allows you to easily and securely connect, manage, and ingest data from millions of globally dispersed devices. IoT Core, in combination with other services on Google Cloud, provides a complete solution for collecting, processing, analyzing, and visualizing IoT data in real-time to support improved operational efficiency.

Question 90:
Your company started working with a cloud service provider, and after a while, they were disappointed with their service and wanted to move to another CSP.

Which of the following can become a problem when changing to a new CSP?

- **Lock-in**
- **Lock-up**
- **Lock-down**
- **Virtualization**

Explanation
https://jaychapel.medium.com/how-much-should-enterprises-worry-about-vendor-lock-in-in-public-cloud-5029bf40fffa

The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud service provider (CSP) technology implementation and cannot easily move to a different vendor without substantial costs or technical incompatibilities.

Types of vendor lock-in risks

The issue with vendor lock-in is the difficulty in moving to another cloud service provider if something goes awry. You hope that this never has to happen, but it's a possibility.

There are four primary lock-in risks that you'll take working with a single cloud provider. These include:

1. Data transfer risk

2. Application transfer risk

3. Infrastructure transfer risk

4. Human resource knowledge risk

Data transfer risk

It is not easy to move your data from one CSP to another.

A myriad of questions will arise during a data migration process, such as:

1. Who is responsible for extracting the data from the cloud databases and data warehouses?

2. In what format will the data be? Will that format work with the new cloud provider, or will significant changes need to be made to the data?

3. How can the data be transferred without loss of application functionality?

4. How long will it take and how much will it cost to move all of this data?

While some industry groups have tried to create standards for data interchange, sometimes it's difficult for companies to implement them due to their unique business requirements.

Application transfer risk

If you build an application on one CSP that leverages many of its offerings, the reconfiguration of this application to run natively on another provider can be an extremely expensive and difficult process.

For instance, let's say you've developed a business intelligence platform on Microsoft Azure. You leverage basic cloud services like compute, storage, databases, and networking. But the app also includes Azure's machine learning, data lake analytics, and bot services.

Can you imagine all the changes you'll have to make to your application if you had to move this to another CSP?

One reason for this difficulty is a lack of standard interfaces and open APIs. Every CSP has their own proprietary specifications and standards, which make it very tough to move from one to another.

Another reason is that technology and customer needs change so rapidly.

You know first hand that your customers and partners continuously demand changes and improvements to your product. The faster that you add and edit features of your cloud-native application, the deeper entrenched you get with your CSP, and the tougher it will be to move to another cloud vendor.

Infrastructure transfer risk

Every major CSP does things a little bit differently.

Virtual machine formats and their associated pricing vary from vendor to vendor, making it difficult to ensure that you have the appropriate resource usage and cost savings if you switch providers.

Database offerings and formats may differ as well.

And one cloud provider may have more attractive offerings in certain infrastructure components, while lacking in other services that you may need.

These differences in the underlying infrastructure result in difficulties moving from one cloud service provider to another.

Human resource knowledge risk

If you've been working with a single CSP, your IT team has likely gained a lot of institutional knowledge about that provider's tools and configurations.

If you have to move your applications to another CSP, it will take time for your engineers to ramp up their knowledge of the new cloud platform. They'll have to learn about new infrastructure formats, implementation processes, and more.

Additionally, any newly required certifications will take a long time to earn.

The knowledge risk is a factor that isn't often thought about, but is just as important as the risks highlighted above.

Question 91:
Which of the following standards is most applicable for a major credit card company?

- **Sarbanes-Oxley Act**
- **HIPAA**
- **PCI-DSS**
- **FISMA**

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

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.

Validation of compliance is performed annually or quarterly better source needed] by a method suited to the volume of transactions handled:

Self-Assessment Questionnaire (SAQ) — smaller volumes;

External Qualified Security Assessor (QSA) — moderate volumes; involves an Attestation on Compliance (AOC);

Firm-specific Internal Security Assessor (ISA) — larger volumes; involves issuing a Report on Compliance (ROC).

Incorrect answers:

FISMA https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

The Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347 (text) (pdf), 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. In FY 2008, federal agencies spent $6.2 billion securing the government's total information technology investment of approximately $68 billion or about 9.2 percent of the total information technology portfolio.

Sarbanes-Oxley Act https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations.

The act, (Pub.L. 107–204 (text) (pdf), 116 Stat. 745, enacted July 30, 2002), also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley or SOX, contains eleven sections that place requirements on all U.S. public company boards of directors and management and public accounting firms. A number of provisions of the Act also apply to privately held companies, such as the willful destruction of evidence to impede a federal investigation.

The law was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The sections of the bill cover responsibilities of a public corporation's board of directors, add criminal penalties for certain misconduct, and require

the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law.

HIPAA https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage. It generally prohibits healthcare providers and healthcare businesses, called covered entities, from disclosing private information to anyone other than a patient and the patient's authorized representatives. It does not restrict patients from receiving information about themselves, prohibit them from voluntarily sharing their private health information however they choose, or – if they disclose private medical information to family members, friends, or other private individuals – legally require those non-covered people to maintain confidentiality.

Question 92:
Which of the following parameters is Nmap helps evade IDS or firewalls?

- **-A**
- **-T**
- **-R**
- **-r**

Explanation
https://nmap.org/book/performance-timing-templates.html

While the fine-grained timing controls discussed in the previous section are powerful and effective, some people find them confusing. Moreover, choosing the appropriate values can sometimes take more time than the scan you are trying to optimize. So Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). ***The first two are for IDS evasion***. Polite mode slows down the scan to use less bandwidth and target machine resources. Normal mode is the default and so -T3 does nothing. Aggressive mode speeds scans up by making the assumption that you are on a reasonably fast and reliable network. Finally insane mode assumes that you are on an extraordinarily fast network or are willing to sacrifice some accuracy for speed.

Incorrect answers:

-A (Aggressive scan options)

This option enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute). More features may be added in the future. The point is to enable a comprehensive set of scan options without people having to remember a large set of flags. However, because script scanning with the default set is considered intrusive, you should not use -A against target networks without permission. This option only enables features, and not timing options (such as -T4) or verbosity options (-v) that you might want as well. Options which require privileges (e.g. root access) such as OS detection and traceroute will only be enabled if those privileges are available.

-R (DNS resolution for all targets)

Tells Nmap to *always* do reverse DNS resolution on the target IP addresses. Normally reverse DNS is only performed against responsive (online) hosts.

-r

Nmap randomizes the port scan order by default to make detection slightly harder. The -r option causes them to be scanned in numerical order instead.

Question 93:
Which of the following is a rootkit that adds additional code or replaces portions of the core operating system to obscure a backdoor on a system?

- **User-mode rootkit.**
- **Hypervisor-level rootkit.**
- **Kernel-level rootkit.**
- **Application-level Rootkit.**

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

Kernel-Level rootkit: Kernel is the core of the Operating System and Kernel Level Rootkits are created by adding additional code or replacing portions of the core operating system, with modified code via device drivers (in Windows) or Loadable Kernel Modules (Linux). Kernel Level Rootkits can have a serious effect on the stability of the system if the kit's code contains bugs. Kernel rootkits are difficult to detect because they have the same privileges of the Operating System, and therefore they can intercept or subvert operating system operations.

Incorrect answers:

Application-level rootkit: Application-level rootkits operate inside the victim computer by changing standard application files with rootkit files, or changing the behaviour of present applications with patches, injected code etc.

Hypervisor-Level rootkit: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware-assisted virtualization technologies). Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

User-mode rootkit: User-mode rootkits run along with other applications as user, rather than low-level system processes. They have a number of possible installation vectors to intercept and modify the standard behavior of application programming interfaces (APIs). Some inject a dynamically linked library (such as a .DLL file on Windows, or a .dylib file on Mac OS X) into other processes, and are thereby able to execute inside any target process to spoof it; others with sufficient privileges simply overwrite the memory of a target application.

Question 94:
The boss has instructed you to test the company's network from the attacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world by using devices such as firewalls, routers, and servers. During this process, you should also external assessment estimates the threat of network security attacks external to the organization.

What type of vulnerability assessment should you perform?

- **External assessment**
- **Passive assessment**
- **Active Assessments**
- **Host-based Assessments**

Explanation
https://info-savvy.com/top-8-most-useful-vulnerability-assessments/

External Assessments

External assessment assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. These types of assessments use external devices like firewalls, routers, and servers. An external assessment estimates the threat of network security attacks external to the organization. it determines how secure the external network and firewall are.

Incorrect answers:

Host-based Assessments

Host-based assessments are a type of security check that involves carrying out a configuration-level check through the command line. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools.

Passive Assessments

Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerability assessments. Even passive assessments provide a list of the users who are recently using the network.

Active Assessments

Active evaluation is a type of vulnerability assessment that uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. These network scanners have the capability to reduce the intrusiveness of the checks they perform.

Question 95:
Which of the following types of attack does the use of Wi-Fi Pineapple belong to run an access point with a legitimate-looking SSID for a nearby business?

- **Wardriving attack**
- **MAC spoofing attack**
- **Phishing attack**
- **Evil-twin attack**

Explanation
https://terranovasecurity.com/wi-fi-pineapple-cyber-security-threat/

A Wi-Fi Pineapple is a wireless auditing platform from Hak5 that allows network security administrators to conduct penetration tests. Pen tests are a type of ethical hacking in which white hat hackers seek out security vulnerabilities that a black hat attacker could exploit. The labels white hat and black hat are derived from old-time Western movies in which the good guys wore white hats and the bad guys wore black hats.

A Wi-Fi Pineapple can also be used as a rogue access point (AP) to conduct man-in-the-middle (MitM) attacks. A MiTM attack is one in which the attacker secretly intercepts and relays messages between two parties that believe they are communicating directly with each other. The inexpensive price and friendly user interface (UI) enable attackers with little technical knowledge to eavesdrop on computing devices using public Wi-Fi networks in order to collect sensitive personal information, including passwords.

Uses of Wi-Fi Pineapple

The Pineapple was originally invented by engineers at Hak5 to perform pen tests and help network administrators audit network security. The AP, which some people think resembles a spider instead of a pineapple, enables network engineers to hack their own network in order to identify vulnerabilities and put mechanisms in place to strengthen the network against potential attackers.

When a Pineapple is used for pen testing, it is referred to as a honeypot. When a Pineapple is used as a rogue AP to conduct MitM security exploits, it is referred to as an evil twin or pineapple sandwich.

Question 96:
Which antenna is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- **Omnidirectional antenna**
- **Parabolic grid antenna**
- **Dipole antenna**
- **Yagi antenna**

Explanation
https://en.wikipedia.org/wiki/Yagi%E2%80%93Uda_antenna

A Yagi–Uda antenna or simply Yagi antenna, is a directional antenna consisting of two or more parallel resonant antenna elements in an end-fire array; these elements are most often metal rods acting as half-wave dipoles. Yagi–Uda antennas consist of a single driven element connected to a radio transmitter and/or receiver through a transmission line, and additional "parasitic elements" with no electrical connection, usually including one so-called reflector and any number of directors. It was invented in 1926 by Shintaro Uda of Tohoku Imperial University, Japan, with a lesser role played by his colleague Hidetsugu Yagi.

Reflector elements (usually only one is used) are slightly longer than the driven dipole and placed behind the driven element, opposite the direction of intended transmission. Directors, on the other hand, are a little shorter and placed in front of the driven element in the intended direction. These parasitic elements are typically off-tuned short-circuited dipole elements, that is, instead of a break at the feedpoint (like the driven element) a solid rod is used. They receive and reradiate the radio waves from the driven element but in a different phase determined by their exact lengths. Their effect is to modify the driven element's radiation pattern. The waves from the multiple elements superpose and interfere to enhance radiation in a single direction, increasing the antenna's gain in that direction.

Also called a beam antenna and parasitic array, the Yagi is very widely used as a high-gain antenna on the HF, VHF and UHF bands. It has moderate to high gain depending on the number of elements present, sometimes reaching as high as 20 dBi, in a unidirectional beam pattern. As an end-fire array, it can achieve a front-to-back ratio of up to 20 dB. It retains the polarization common to its elements, usually linear polarization (its elements being half-wave dipoles). It is relatively lightweight, inexpensive and simple to construct.The bandwidth of a Yagi antenna, the frequency range over which it maintains its gain and feedpoint impedance, is narrow, just a few percent of the center frequency,

decreasing for models with higher gain, making it ideal for fixed-frequency applications. The largest and best-known use is as rooftop terrestrial television antennas, but it is also used for point-to-point fixed communication links, in radar antennas, and for long distance shortwave communication by shortwave broadcasting stations and radio amateurs.

Question 97:
WPS is a rather troubled wireless network security standard. While it can make your life easier, it is also vulnerable to attacks. An attacker within radio range can brute-force the WPS PIN for a vulnerable access point, obtain WEP or WPA passwords, and likely gain access to the Wi-Fi network. However, first, the attacker needs to find a vulnerable point.

Which of the following tools is capable of determining WPS-enabled access points?

- **wash**
- **net view**
- **macof**
- **ntptrace**

Explanation
https://ru.wikipedia.org/wiki/Wi-Fi_Protected_Setup

WiFi Protected Setup (WPS) is a computing standard created by the WiFi Alliance to ease a wireless home network setup and security. WPS contains an authentication method called "external registrar" that only requires the router's PIN.

The WiFi Protected Setup (WPS) PIN is susceptible to a brute force attack. A design flaw in the WPS specification for the PIN authentication significantly reduces the time required to brute force the entire PIN because it allows an attacker to know when the first half of the eight-digit PIN is correct. The lack of a proper lock-out policy after a certain number of failed attempts to guess the PIN on many wireless routers makes this brute force attack that much more feasible. Once on the network, the attacker can monitor traffic and mount further attacks.

Wash https://en.kali.tools/?p=341

Wash is a utility for identifying WPS enabled access points. It can survey from a live interface or it can scan a list of pcap files.It is an auxiliary tool designed to display WPS enabled Access Points and their main characteristics.

Incorrect answers:

net view

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875576(v=ws.11)

Displays a list of domains, computers, or resources that are being shared by the specified computer. Used without parameters, net view displays a list of computers in your current domain.

Macof https://linux.die.net/man/8/macof

macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

Ntptrace https://www.ibm.com/docs/en/aix/7.2?topic=n-ntptrace-command

Traces a chain of Network Time Protocol (NTP) hosts back to their master time source.

Question 98:
Identify technique for securing the cloud resources according to describe below:

This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. When using this technique imposed conditions such that employees can access only the resources required for their role.

- **Container technology**
- **Zero trust network**
- **Serverless computing**
- **DMZ**

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

Zero Trust Network Access (ZTNA) is a category of technologies that provides secure remote access to applications and services based on defined access control policies. Unlike VPNs, which grant complete access to a LAN, ZTNA solutions default to deny, providing only the access to services the user has been explicitly granted.

Incorrect answers:

DMZ https://en.wikipedia.org/wiki/DMZ_(computing)

DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

Serverless computing https://en.wikipedia.org/wiki/Serverless_computing

Serverless computing is a cloud computing execution model in which the cloud provider allocates machine resources on demand, taking care of the servers on behalf of their customers. Serverless computing does not hold resources in volatile memory; computing is rather done in short bursts with the results persisted to storage. When an app is not in use, there are no computing resources allocated to the app. Pricing is based on the actual amount of resources consumed by an application. It can be a form of utility computing. "Serverless" is a misnomer in the sense that servers are still used by cloud service providers to execute code for developers.

Container technology

Container technology, also simply known as just a container, is a method to package an application so it can be run, with its dependencies, isolated from other processes. The major public cloud computing providers, including Amazon Web Services, Microsoft Azure and Google Cloud Platform have embraced container technology, with container software having names including the popular choices of Docker, Apache Mesos, rkt (pronounced “rocket”), and Kubernetes.

Question 99:
Identify the type of SQLi by description:

This type of SQLi doesn't show any error message. Its use may be problematic due to as it returns information when the application is given SQL payloads that elicit a true or false response from the server. When the attacker uses this method, an attacker can extract confidential information by observing the responses.

- **Union SQLi**
- **Error-based SQLi**
- **Blind SQLi**
- **Out-of-band SQLi**

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

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

Incorrect answers:

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.

Out-of-band SQLi

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.

Error-based SQLi

Error-based SQL injections are exploited by triggering errors in the database when invalid inputs are passed to it. The error messages can be used to return the full query results or gain information on how to restructure the query for further exploitation.

Question 100:
Which of the following frameworks contains a set of the most popular tools that facilitate your tasks of collecting information and data from open sources?

- **WebSploit Framework**
- **BeEF**
- **OSINT framework**
- **Speed Phish Framework**

Explanation
https://osintframework.com/

This tool is mainly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.

It also provides an excellent classification of all existing intel sources, making it an excellent resource for knowing what infosec areas you are neglecting to explore or the next suggested OSINT steps for your investigation.

Incorrect answers:

WebSploit Framework https://sourceforge.net/projects/websploit/

This is an open source project which is used to scan and analysis remote system in order to find various type of vulnerabilities. This tool is very powerful and support multiple vulnerabilities.

BeEF https://beefproject.com/

This is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Speed Phish Framework https://github.com/tatanus/SPF

SPF (SpeedPhish Framework) is a python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.