Question 1:
Alex works as a network administrator at ClassicUniversity. There are many Ethernet ports are available for professors and authorized visitors (but not for students) on the university campus.
However, Alex realized that some students connect their notebooks to the wired network to have Internet access. He identified this when the IDS alerted for malware activities in the network. What should Alex do to avoid this problem?

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

Explanation
https://en.wikipedia.org/wiki/IEEE_802.1X
The correct answer is to "Use the 802.1x protocol" because the IEEE 802.1X standard defines an access control and authentication protocol that restricts the rights of unauthorized computers connected to the switch. And this will help Alex solve the problem with the students.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.11 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.11, which is known as "EAP over LAN" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004. The EAPOL was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010 to support service identification and optional point to point encryption over the internal LAN segment.

Question 2:
An attacker stole financial information from a bank by compromising only a single server. After that, the bank decided to hire a third-party organization to conduct a full security assessment. Cybersecurity specialists have been provided with information about this case, and they need to provide an initial recommendation. Which of the following will be the best recommendation?

- **Move the financial data to another server on the same IP subnet.**
- **Require all employees to change their passwords immediately.**
- **Place a front-end web server in a demilitarized zone that only handles external web traffic.**
- **Issue new certificates to the web servers from the root certificate authority.**

Explanation
https://en.wikipedia.org/wiki/DMZ_(computing)
The best solution would be to use a DMZ because it adds an additional layer of security to an organization's local area network: 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 is seen as not belonging to either party bordering it. This metaphor applies to the computing use as the DMZ acts as a gateway to the public Internet. It is neither as secure as the internal network, nor as insecure as the public internet.

In this case, the hosts most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, Web and Domain Name System (DNS) servers. Because of the increased potential of these hosts suffering an attack, they are

placed into this specific subnetwork in order to protect the rest of the network should any of them become compromised.

Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network. Similarly, communication between hosts in the DMZ and to the external network is also restricted to make the DMZ more secure than the Internet and suitable for housing these special purpose services. This allows hosts in the DMZ to communicate with both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients, and another firewall would perform some level of control to protect the DMZ from the external network.

Question 3:
Which of the following components of IPsec provides confidentiality for the content of packets?

- **AH**
- **IKE**
- **ESP**
- **ISAKMP**

Explanation
https://en.wikipedia.org/wiki/IPsec#Encapsulating_Security_Payload

Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. It provides origin authenticity through source authentication, data integrity through hash functions, and confidentiality through encryption protection for IP packets. ESP also supports encryption-only and authentication-only configurations but using encryption without authentication is strongly discouraged because it is insecure.

Incorrect answers:

AH https://en.wikipedia.org/wiki/IPsec#Authentication_Header

Authentication Header (AH) is a member of the IPsec protocol suite. AH ensures connectionless integrity by using a hash function and a secret shared key in the AH algorithm. AH also guarantees the data origin by authenticating IP packets.

IKE https://en.wikipedia.org/wiki/Internet_Key_Exchange

Internet Key Exchange (IKE, sometimes IKEv1 or IKEv2, depending on the version) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication – either pre-shared or distributed using DNS (preferably with DNSSEC) – and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

ISAKMP https://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol

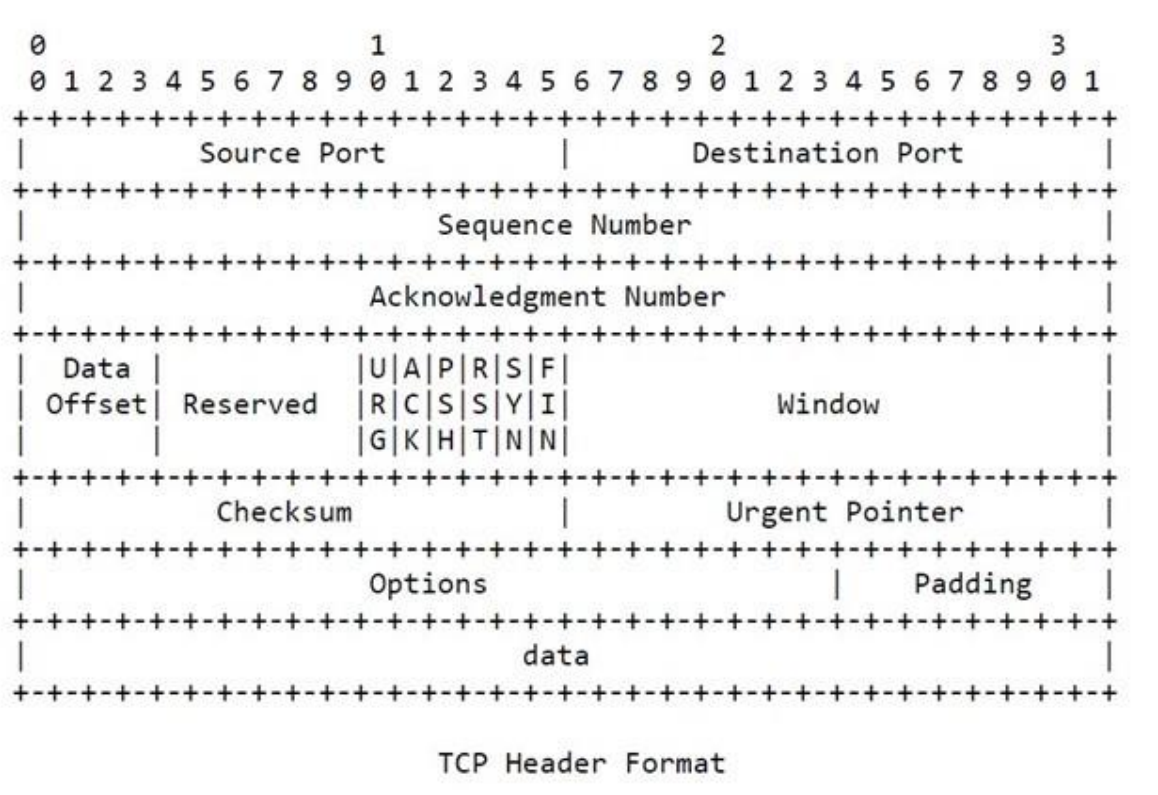
Internet Security Association and Key Management Protocol (ISAKMP) is a protocol defined by RFC 2408 for establishing Security association (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK) provide authenticated keying material for use with ISAKMP. For example: IKE describes a protocol using part of Oakley

and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

Question 4:
Transmission Control Protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. A TCP segment consists of a segment header and a data section. The segment header contains 10 mandatory fields and an optional extension field. Which of the suggested fields is not included in the TCP segment header?

- **Checksum**
- **Sequence Number**
- **Source Port**
- **Source IP address**

Explanation
https://datatracker.ietf.org/doc/html/rfc793



TCP Header Format

Source Port (16 bits)

Identifies the sending port.

Sequence Number (32 bits)

· If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number plus 1.

· If the SYN flag is clear (0), then this is the accumulated sequence number of the first data byte of this segment for the current session.

Checksum (16 bits)

The 16-bit checksum field is used for error-checking of the TCP header, the payload and an IP pseudo-header. The pseudo-header consists of the source IP address, the destination IP

address, the protocol number for the TCP protocol (6) and the length of the TCP headers and payload (in bytes).

Question 5:
Identify the way to achieve chip-level security of an IoT device?

- **Changing the password of the router**
- **Turning off the device when not needed or not in use**
- **Closing insecure network services**
- **Encrypting the JTAG interface**

Explanation
The quick way is to remove all non-chip-level options. Disabling services, disabling the device, and changing the default password on the router is obviously not included in this level, so one option remains. But this is not fun!

Loooong way

The problem with all IoT devices is that most sensitive information about a device, including certificates, keys, and communication protocols, is usually stored in poorly secured flash memory. Anyone with access to an IoT device and some basic knowledge of hacking hardware can easily access the firmware to search for data.

JTAG is a common hardware interface that provides your computer to communicate directly with the chips aboard. It was originally developed by a consortium, the Joint (European) Test Access Group, in the mid-80s to address the increasing difficulty of testing printed circuit boards (PCBs). JTAG has been in widespread use ever since it was included in the Intel 80486 processor in 1990 and codified as IEEE 1491 that same year. Today JTAG is used for debugging, programming, and testing on virtually ALL embedded devices.

An attacker with JTAG access could:

· Read and Write from memory;

· Pause execution of firmware (set breakpoints and watchpoints);

· Patch instructions or data into memory;

· Inject instructions directly into the pipeline of the target chip (without modifying memory);

· Extract Firmware (for reverse engineering/vulnerability research);

· Bypass protection mechanisms (encryption checks, password checks, checksums, you name it);

· Find hidden JTAG functionality that might do far more than we imagine;

· ...do whatever he wants, really.

JTAG is a compelling interface to embedded devices. Developers who write code deployed on embedded systems are often unaware that this level of access exists. There are systems where the firmware developers seemed to have poured hours into encrypting and protecting data in their code without realizing it can be subverted trivially with hardware-level access.

Manufacturers are aware of this issue and often take steps to restrict access to JTAG. Protection methods can be different: hiding traces on the board or completely removing pins. During manufacture, the wires leading to the interface can be intentionally damaged. These

methods are somewhat effective, but a skilled attacker with a soldering iron in hand can almost always repair the damage. Some standards recommend encryption and cryptographic authentication, but in practice, these methods are rarely used.

NOTE: Technically, "Encrypting the JTAG interface" is not entirely correct. This is one of the ways, but far from the most effective and often used. Yes, this is a serious vulnerability, but the chance of its occurrence is tiny since the intruder will have to gain physical access to the device somehow. Plus, there are much more convenient attack surfaces that you should be wary of.

Question 6:
One of the most popular tools in the pentester's arsenal - John the Ripper is designed for...

- **Discover hosts and services on a computer network by sending packets and analyzing the responses.**
- **Automation of the process of detecting and exploiting the SQL injection vulnerability.**
- **Test password strength, brute-force encrypted or hashed passwords, and crack passwords via dictionary attacks.**
- **Search for various default and insecure files, configurations, and programs on any type of web servers.**

Explanation
https://en.wikipedia.org/wiki/John_the_Ripper
John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

Question 7:
In what type of testing does the tester have some information about the internal work of the application?

- **Announced**
- **Black-box**
- **White-box**
- **Grey-box**

Explanation
Gray box refers to the testing of software where there is some limited knowledge of its internal workings. Gray box testing is an ethical hacking technique where hackers have to use limited information to identify a target's security network's strengths and weaknesses.

Gray box is the hybrid of white box testing, where the tester examines the internal logic and structure of the software’s code, and black-box testing, where the tester knows nothing about the software’s code. To understand gray box testing, we must first understand black box testing and white box testing.

Black Box and White Box Testing

Black box testing looks at nothing more than inputs by the user and what output the software produces given those inputs. Black box testing does not require any knowledge of programming language or other technical details. It is a type of high-level testing used in

system testing and acceptance testing. Software engineers require a software requirement specification (SRS) document to perform black-box testing. This testing takes an end-user perspective where the black box tester does not know how the outputs are generated from the inputs.

White box testing requires in-depth knowledge of the techniques and platforms used to build software, including the relevant programming language. It is a type of low-level testing used in unit testing and indication testing. Software engineers need to understand the programming language used to create the application to understand its source code. White box testing's primary purposes are to strengthen security, examine how inputs and outputs flow through the application, and improve design and usability. When a white box tester does not get the expected output from a given input, the result is considered a bug that needs to be fixed.

How Gray Box Testing Works

Gray box testing includes both black and white box testing components to get a better result than either. Both end-users and developers perform gray box testing with limited (partial) knowledge of an application's source code. Gray box testing can be manual or automated. It is more comprehensive and time-consuming than black-box testing, but not as comprehensive or time-consuming as white-box testing. Gray box testers require detailed design documents.

Gray box testing involves identifying inputs, outputs, major paths, and subfunctions. It then develops inputs and outputs for subfunctions, executes test cases for subfunctions, and verifies those results.

Question 8:
The analyst needs to evaluate the possible threats to Blackberry phones for third-party company. To do this, he will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defences and gain access to the corporate network. Which of the following tools is best suited for the analyst for this task?

- **BBProxy**
- **Paros Proxy**
- **BBCrack**
- **Blooover**

Explanation
Blackjacking is the act of hijacking a BlackBerry connection. Attackers make use of the BlackBerry environment to bypass traditional security. They attack the host of the network, usually with the BBProxy tool.

BlackBerry Attack Toolkit

The BlackBerry Attack Toolkit includes the BBProxy and BBScan tools, as well as the necessary Metasploit patches to exploit Web site vulnerabilities. The BBProxy tool allows the attacker to use a BlackBerry device as a proxy between the Internet and the internal network. The attacker either installs BBProxy on a user's BlackBerry or sends it in an e-mail attachment. Once activated, it establishes a covert channel between attackers and compromised hosts on improperly secured enterprise networks. BBScan is a BlackBerry port scanner that looks for open ports on the device to attack.

BlackBerry Attachment Service Vulnerability

The BlackBerry Attachment Service in the BlackBerry Enterprise Server uses a GDI (Graphics Device Interface) component to convert images into a format viewable on

BlackBerry devices. There is, however, a vulnerability in the GDI component of Windows while processing Windows Metafile (WMF) and Enhanced Metafile (EMF) images. This vulnerability could allow an attacker to run arbitrary code on a computer running the BlackBerry Attachment Service. Attackers can exploit this vulnerability with specially made image files.

TeamOn Import Object ActiveX Control Vulnerability

The BlackBerry Internet Service is designed to work with T-Mobile My E-mail to give BlackBerry device users secure and direct access to any combination of registered enterprise, proprietary, POP3, and IMAP e-mail accounts on their BlackBerry devices using a single user login account. A vulnerability exists in the TeamOn Import Object Microsoft ActiveX control used by BlackBerry Internet Service 2.0. While using Internet Explorer to view the BlackBerry Internet Service or T-Mobile My E-mail Web sites, if the user attempts to install and run the TeamOn Import Object ActiveX control, an exploitable buffer overflow may occur.

Denial of Service in the BlackBerry Browser

A Web site creator with malicious intent may insert a long string value within the link to a Web page. If the user accesses the link using the BlackBerry Browser, a temporary denial of service may occur, and the BlackBerry device may become slow or stop responding altogether.

Question 9:
In order to prevent collisions and protect password hashes from rainbow tables, Maria, the system administrator, decides to add random data strings to the end of passwords before hashing. What is the name of this technique?

- **Stretching**
- **Salting**
- **Extra hashing**
- **Masking**

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

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

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

Question 10:
Maria, the leader of the Blue Team, wants to use network traffic analysis to implement the ability to detect an intrusion in her network of several hosts quickly. Which tool is best suited to perform this task?

- **Firewalls**
- **HIDS**
- **NIDS**
- **Honeypot**

Explanation
https://en.wikipedia.org/wiki/Intrusion_detection_system#Network_intrusion_detection_systems
Correct answer NIDS because a discovery system is required for large network environments. HIDS can meet such requirements only in conjunction with NIDS.

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

Incorrect answers:

HIDS https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

A host-based intrusion detection system (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces.

Firewall https://en.wikipedia.org/wiki/Firewall_(computing)

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Honeypot https://en.wikipedia.org/wiki/Honeypot_(computing)

A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site that seems to contain information or a resource of value to attackers, but actually, is isolated and monitored and enables blocking or analyzing the attackers.

Question 11:
Identify a component of a risk assessment?

- **Physical security**
- **Logical interface**
- **DMZ**
- **Administrative safeguards**

Explanation
A complete and compliant risk assessment must include four distinct components:

1. Technical Safeguards

Technical safeguards are those that protect the aspects of how you're storing your personal health information and are generally tested by running a vulnerability scan. The vulnerability scan is an automated test that identifies network security weaknesses.

2. Organizational safeguards

Organizational safeguards primarily address the "minimum necessity rule." This Rule is designed to ensure and determine who has access to specific data and to consider whether it is required or necessary to perform their duties. If any person has more access than they need, you've created an organizational vulnerability.

3. Physical safeguards

Physical safeguards speak to the physical protection of information. You are the custodian of privileged patient information and are responsible for its care. This component includes precautions that defend against physical and environmental hacking, such as building security, key card access, off-site data replication and recovery, and firewall protection, to name a few.

4. Administrative safeguards

Administrative safeguards are the protection of information from a legal perspective. They include such things as business associate agreements, employee confidentiality agreements, background checks, termination checklists, and the implementation of formal policies and procedures. It's critical to be able to administratively ensure that you have proper documentation and processes in place to terminate an employee's access and maintain compliance, especially in an environment where technology plays such a large part.

Question 12:
Which of the following types of keys does the Heartbleed bug expose to the Internet, making exploiting any compromised system very easy?

- **Shared**
- **Private**
- **Root**
- **Public**

Explanation
https://en.wikipedia.org/wiki/Heartbleed
Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. Thus, the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.

Heartbleed is registered in the Common Vulnerabilities and Exposures database as CVE-2014-0160. The federal Canadian Cyber Incident Response Centre issued a security bulletin advising system administrators about the bug. A fixed version of OpenSSL was released on 7 April 2014, on the same day Heartbleed was publicly disclosed.

As of May 20, 2014, 1.5% of the 800,000 most popular TLS-enabled websites were still vulnerable to Heartbleed. As of June 21, 2014, 309,197 public web servers remained vulnerable. As of January 23, 2017, according to a report from Shodan, nearly 180,000

internet-connected devices were still vulnerable. As of July 6, 2017, the number had dropped to 144,000, according to a search on shodan.io for "vuln:cve-2014-0160". As of July 11, 2019, Shodan reported that 91,063 devices were vulnerable. The U.S. was first with 21,258 (23%), the top 10 countries had 56,537 (62%), and the remaining countries had 34,526 (38%). The report also breaks the devices down by 10 other categories such as organization (the top 3 were wireless companies), product (Apache httpd, nginx), or service (https, 81%).

At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft **of the servers' private keys and users' session cookies and passwords**.

Question 13:
Shortly after replacing the outdated equipment, John, the company's system administrator, discovered a leak of critical customer information. Moreover, among the stolen data was the new user's information that excludes incorrect disposal of old equipment. IDS did not notice the intrusion, and the logging system shows that valid credentials were used. Which of the following is most likely the cause of this problem?

- **Default Credential**
- **NSA backdoor**
- **Industrial Espionage**
- **Zero-day vulnerabilities**

Explanation
https://en.wikipedia.org/wiki/Default_Credential_vulnerability
A Default Credential vulnerability is a type of vulnerability that is most commonly found to affect the devices like modems, routers, digital cameras, and other devices having some pre-set (default) administrative credentials to access all configuration settings. The vendor or manufacturer of such devices uses a single pre-defined set of admin credentials to access the device configurations, and any potential hacker can misuse this fact to hack such devices, if those credentials are not changed by the consumers.

NOTE: Yeap, it's that simple. It is more likely that the problem is a simple mistake or incompetence of an employee, which was used by an ordinary fraudster, than a full-fledged attack by real hackers or a conspiracy.

Question 14:
An attacker gained access to a Linux host and stolen the password file from /etc/passwd. Which of the following scenarios best describes what an attacker can do with this file?

- **Nothing because he cannot read the file because it is encrypted.**
- **The attacker can perform actions as a user because he can open it and read the user ids and corresponding passwords.**
- **Nothing because the password file does not contain the passwords themselves.**
- **The attacker can perform actions as root because the file reveals the passwords to the root user only.**

Explanation
https://en.wikipedia.org/wiki/Passwd#Password_file
The /etc/passwd file is a text-based database of information about users that may log into the system or other operating system user identities that own running processes.

In many operating systems this file is just one of many possible back-ends for the more general passwd name service.

The file's name originates from one of its initial functions as it contained the data used to verify passwords of user accounts. However, on modern Unix systems the security-sensitive

password information is instead often stored in a different file using shadow passwords, or other database implementations.

The /etc/passwd file typically has file system permissions that allow it to be readable by all users of the system (world-readable), although it may only be modified by the superuser or by using a few special purpose privileged commands.

The /etc/passwd file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons. The ordering of the records within the file is generally unimportant.

Question 15:
What is the minimum number of network connections needed for a multi-homed firewall?

- **2**
- **4**
- **5**
- **3**

Explanation
According to EC-Council training materials: A multi-homed firewall is a node with multiple NICs that connects to two or more networks. A multi-homed firewall helps in increasing the efficiency and reliability of an IP network. The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the organizations' specific security objectives.

Question 16:
Identify the type of attack according to the following scenario:
Ivan, a black-hat hacker, initiates an attack on a certain organization. In preparation for this attack, he identified a well-known and trust website that employees of this company often use. In the next step, Ivan embeds an exploit into the website that infects the target systems of employees when using the website. After this preparation, he can only wait for the successful execution of his attack.

- **Spear Phishing**
- **Watering Hole**
- **Shellshock**
- **Heartbleed**

Explanation
https://en.wikipedia.org/wiki/Watering_hole_attack
A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

The name watering hole attack is inspired by predators in the natural world who lurk near watering holes, looking for opportunities to attack desired prey. In a watering hole attack, the predator lurks near niche websites popular with the target prey, looking for opportunities to infect the websites with malware or malvertisements that will make the target vulnerable.

Incorrect answers:

Heartbleedhttps://en.wikipedia.org/wiki/Heartbleed

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client.

It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. Thus, the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.

Spear Phishing https://en.wikipedia.org/wiki/Phishing#Spear_phishing

Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and recently bought online. The attackers then disguise themselves as trustworthy friends or entities to acquire sensitive information, typically through email or other online messaging. This is the most successful form of acquiring confidential information on the internet, accounting for 91% of attacks.

Shellshock https://en.wikipedia.org/wiki/Shellshock_(software_bug)

Shellshock, also known as Bashdoor, is a family of security bugs in the Unix Bash shell, the first of which was disclosed on 24 September 2014. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access to many Internet-facing services, such as web servers, that use Bash to process requests.

Question 17:
Which of the following documents describes the specifics of the testing, the associated violations and essentially protects both the organization's interest and third-party penetration tester?

- **Project Scope**
- **Service Level Agreement**
- **Non-Disclosure Agreement**
- **Rules of Engagement**

Explanation
Rules of engagement (ROE) are the formal permissions to conduct a penetration test. They provide certain rights and restrictions to the test team for performing the test and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques. Some of the directives that should be clearly spelled out in RoE before you start the penetration test are as follows:

· The type and scope of testing

· Client contact details

· Client IT team notifications

· Sensitive data handling

· Status meeting and reports

Question 18:
In what type of attack does the attacker forge the sender's IP address to gain access to protected systems and confidential data?

- **IP fragmentation attack**
- **IP Spoofing**
- **Source Routing**
- **IP forwarding**

Explanation

https://en.wikipedia.org/wiki/IP_address_spoofing
Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity. It's one of many tools hackers use to access computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks. Of the several types of spoofing, IP spoofing is the most common.

The data transmitted over the internet is first broken into multiple packets, and those packets are transmitted independently and reassembled at the end. Each packet has an IP (Internet Protocol) header that contains information about the packet, including the source IP address and the destination IP address.

In IP spoofing, a hacker uses tools to modify the packet header's source address to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

Incorrect answers:

IP fragmentation attack https://en.wikipedia.org/wiki/IP_fragmentation_attack

IP fragmentation attacks are a common form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms.

Understanding the attack starts with understanding the process of IP fragmentation, a communication procedure in which IP datagrams are broken down into small packets, transmitted across a network, and then reassembled back into the original datagram.

Fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process. This limit is known as the maximum transmission unit (MTU). If a datagram is being sent that is larger than the receiving server’s MTU, it must be fragmented to be transmitted completely.

Source Routing https://en.wikipedia.org/wiki/Source_routing

Source routing is a feature of the IP protocol which allows the sender of a packet to specify which route the packet should take on the way to its destination (and on the way back). Source routing was originally designed to be used when a host did not have proper default routes in its routing table.

To find the route that packets take through your network, attackers use IP source route attacks. The attacker sends an IP packet and uses the response from your network to get information about the operating system of the target computer or network device.

IP forwarding

If you want to turn your computer into a router or Internet gateway (and maybe even into a VPN server), you need to enable IP-forwarding, which will allow you to redirect IP packets from one network interface to another. In other words, IP-forwarding is the property of the operating system to accept incoming network packets on one interface and forward them further if they are not intended for the system itself and must be transmitted to another network.

Question 19:
Shellshock is a serious bug in the Bash command-line interface shell that allows an attacker to execute commands by gaining unauthorized access to computer systems.

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

What is the result of executing this query on a vulnerable host?

- **Display of the contents of the passwd file.**
- **Copying the contents of the passwd file**
- **Deleting the passwd file.**
- **Creating a passwd file.**

Explanation
https://blog.cloudflare.com/inside-shellshock/
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form: `() {:;}; /bin/cat /etc/passwd` That reads the password file */etc/passwd*, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

Question 20:
Which of the following is a vulnerability in modern processors such as Intel, AMD and ARM using speculative execution?

- **Launch Daemon**
- **Spectre and Meltdown**
- **Application Shimming**
- **Named Pipe Impersonation**

Explanation
https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

Incorrect answers:

Named Pipe Impersonation https://en.wikipedia.org/wiki/Named_pipe#In_Windows

In Windows OS, named pipes are used to provide legitimate communication between running processes. In this technique, the messages are exchanged between the processes using a file. For example, if process A wants to send a message to another process B, then process A writes the message to a file and process B reads the message from that file. Attackers often exploit this technique to escalate their privileges on the victim system to a user account with higher access privileges.

In any Windows system, when a process creates a pipe, it will act as a pipe server. If any other process wants to communicate with this process, it will connect to this pipe and it becomes a pipe client. When a client connects to the pipe, the pipe server can utilize the access privileges and security context of the pipe client. Attackers exploit this feature by creating a pipe server with fewer privileges and trying to connect with a client with higher privileges than the server.

Attackers use tools such as Metasploit to perform named pipe impersonation on a target host. Attackers exploit vulnerabilities that exist in the target remote host to obtain an active session and use Metasploit commands such as getsystem to gain administrative-level privileges and extract password hashes of the admin/user accounts.

Application Shimming https://en.wikipedia.org/wiki/Shim_(computing)

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10.

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as necessary in order to communicate with the OS.

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc. Shims can also be abused to establish persistence by continuously being invoked by affected programs.

Launch Daemon https://en.wikipedia.org/wiki/Daemon_(computing)

In the context of this question, we are talking about one of the methods of Privilege Escalation.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Adversaries may create or modify launch daemons to repeatedly execute malicious payloads as part of persistence. Per Apple’s developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in /System/Library/LaunchDaemons and /Library/LaunchDaemons. These LaunchDaemons have property list files which point to the executables that will be launched.

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories. The daemon name may be disguised by using a name from a related operating system or benign software. Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

Question 21:
Buffer overflow mainly occurs when a created memory partition (or buffer) is written beyond its intended boundaries. If an attacker manages to do this from outside the program, this can cause security problems since it can potentially allow them to manipulate arbitrary memory cells, although many modern operating systems protect against the worst cases of this. What programming language is this example in?

```
char a[4];
strcpy(a,"a string longer than 4 characters");
printf("%s\n",a[6]);
```

- **SQL**
- **Java**
- **C**
- **HTML**

Explanation
https://en.wikipedia.org/wiki/Buffer_overflow
Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows but requires additional code and processing time.

NOTE: /*a place for a joke about a programming language*/

Question 22:
The network elements of the telecom operator are located in the data center under the protection of firewalls and intrusion prevention systems. Which of the following is true for additional security measures?

- **No additional measures are required, since the attacker does not have physical access to the data center equipment.**
- **Firewalls and intrusion detection systems are sufficient to ensure complete security.**
- **Periodic security checks and audits are required. Access to network elements should be provided by user IDs with strong passwords.**
- **No additional measures are required since attacks and downtime are inevitable, and a backup site is required.**

Explanation
When answering this question, we will start with incorrect answers.

«No additional measures are required, since the attacker does not have physical access to the data center equipment.» incorrect because firewalls and IPS will not be able to provide adequate protection. It only provides monitors and controls incoming and outgoing network traffic.

«**No additional measures are required since attacks and downtime are inevitable, and a backup site is required.**» incorrect because the attack can be carried out over the network.

«Firewalls and intrusion detection systems are sufficient to ensure complete security.» this option might seem correct if there was no better option.

«**Periodic security checks and audits are required. Access to network elements should be provided by user IDs with strong passwords**.». This answer is most appropriate as user ids and strong passwords add an extra layer of security. Regular security tests and audits will help find vulnerabilities and fix them, increasing the reliability of the system.

Question 23:
What is the name of the practice of collecting information from published or otherwise publicly available sources?

- **Human intelligence**
- **Artificial intelligence**
- **Open-source intelligence**
- **Social intelligence**

Explanation
https://en.wikipedia.org/wiki/Open-source_intelligence
Open-source intelligence (OSINT) is a multi-method (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or collective intelligence.

Incorrect answers:

Human intelligence

https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)

Human intelligence (abbreviated HUMINT and is pronounced as hyoo-mint) is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines such as signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT).

NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources." Typical HUMINT activities consist of interrogations and conversations with persons having access to information.

Social intelligence https://en.wikipedia.org/wiki/Social_intelligence

Social intelligence is the capacity to know oneself and to know others. Social Intelligence develops from experience with people and learning from success and failures in social settings. It is more commonly referred to as "tact", "common sense", or "street smarts".

Artificial intelligence https://en.wikipedia.org/wiki/Artificial_intelligence

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

Question 24:
Black-hat hacker Ivan created a fraudulent website to steal users' credentials. What of the proposed tasks does he need to perform so that users are redirected to a fake one when entering the domain name of a real site?

- **ARP Poisoning**
- **SMS phishing**
- **MAC Flooding**
- **DNS spoofing**

Explanation
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).

Incorrect answers:

ARP Poisoning 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.

SMS phishing https://en.wikipedia.org/wiki/Phishing#SMS_phishing

SMS phishing or smishing is conceptually similar to email phishing, except attackers use cell phone text messages to deliver the "bait". Smishing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data; often, credentials to other websites or services. Furthermore, due to the nature of mobile browsers, URLs may not be fully displayed; this may make it more difficult to identify an illegitimate logon page. As the mobile phone market is now saturated with smartphones which all have fast internet connectivity, a malicious link sent via SMS can yield the same result as it would if sent via email. Smishing messages may come from telephone numbers that are in a strange or unexpected format.

MAC Flooding https://en.wikipedia.org/wiki/MAC_flooding

A media access control attack or MAC flooding is a technique employed to compromise the security of network switches. The attack works by forcing legitimate MAC table contents out of the switch and forcing a unicast flooding behavior potentially sending sensitive information to portions of the network where it is not normally intended to go.

Question 25:
The flexible SNMP architecture allows you to monitor and manage all network devices from a single console. The data exchange is based on the Protocol Data Unit (PDU). There are 7 PDUs in the latest version of the SNMP protocol. Which of them sends a notification about the past event immediately, without waiting for the manager's request, and does not need confirmation of receipt?

- **GetRequest**
- **GetNextRequest**
- **Trap**
- **InformRequest**

Explanation
https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN). The purpose of SNMP is to provide network devices such as routers, servers, and printers with a common language for sharing information with a network management system (NMS).

There are multiple versions of the SNMP protocol, and SNMP is so popular that most network devices come pre-bundled with SNMP Agents. However, to make use of the protocol, network administrators must first change the default configuration settings of their network devices so SNMP Agents can communicate with the network's management system.

SNMP is part of the original Internet Protocol Suite defined by the Internet Engineering Task Force (IETF). The most recent version of the protocol, SNMPv3, includes security mechanisms for authentication, encryption, and access control.

SNMP can perform many functions, using a blend of push and pull communications between network devices and the management system. It can issue read or write commands, such as resetting a password or changing a configuration setting. It can also report back how much bandwidth, CPU, and memory are in use, with some SNMP managers automatically sending the administrator an email or text message alert if a predefined threshold is exceeded.

Most of the time, SNMP functions in an asynchronous model, with the SNMP manager's communication and the agent sending a response. These commands and messages, typically transported over User Datagram Protocol (UDP) or Transmission Control Protocol/Internet Protocol (TCP/IP), are known as protocol data units (PDUs):

· GETRequest Generated by the SNMP manager and sent to an agent to obtain the value of a variable, identified by its OID, in a MIB;

· RESPONSE Sent by the agent to the SNMP manager, issued in reply to a GETRequest, GETNEXTRequest, GETBULKRequest, and a SETRequest. Contains the values of the requested variables;

· GETNEXTRequest Sent by the SNMP manager to the agent to retrieve the values of the next OID in the MIB's hierarchy;

· GETBULKRequest Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, extensive tables;

· SETRequest Sent by the SNMP manager to the agent to issue configurations or commands;

· TRAP An asynchronous alert sent by the agent to the SNMP manager to indicate a significant event, such as an error or failure, has occurred;

· INFORMRequest An asynchronous alert similar to a TRAP requires confirmation of receipt by the SNMP manager.

Question 26:
The Domain Name System (DNS) is the phonebook of the Internet. When a user tries to access a web address like "example.com", web browser or application performs a DNS

Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which the web browser can connect to. Which of the proposed tools allows you to set different DNS query types and poll arbitrarily specified servers?

- **Nikto**
- **Wireshark**
- **Nslookup**
- **Metasploit**

Explanation

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

nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

In general, there are two ways of resolving a host or a domain name to an IP address, using the domain name system – a Recursive query and a non-Recursive query.

· ***The Recursive query*** is, when a DNS client directly gets the IP address of a domain, by asking the name server system to perform the complete translation.

For example: # nslookup -recursive www.udemy.com

· ***The non-Recursive query*** is, when a DNS client contacts the name servers, one by one, until it finds the server, containing the needed information.

For example: # nslookup -norecursive www.udemy.com

Question 27:

Which of the following is correct?

- **Sniffers operate on Layer 3 of the OSI model.**
- **Sniffers operate on both Layer 2 & Layer 3 of the OSI model.**
- **Sniffers operate on Layer 2 of the OSI model.**
- **Sniffers operate on Layer 4 of the OSI model.**

Explanation

Protocol analyzers (or sniffers) are powerful programs that work by placing the host system's network card into promiscuous mode, thereby allowing it to receive all of the data it sees in that particular collision domain. Passive sniffing is performed when a user is on a hub. When using a hub, all traffic is sent to all ports; thus, all a security professional or attacker has to do is start the sniffer and wait for someone on the same collision domain to begin transmitting data. A collision domain is a shared network segment but not bridged or switched; packets collide because users share the same bandwidth.

Sniffing performed on a switched network is known as active sniffing because it switches segment traffic and knows which particular port to send traffic. While this feature adds much-needed performance, it also raises a barrier when sniffing all potential switched ports. One way to overcome this impediment is to configure the switch to mirror a port. Attackers may not have this capability, so their best hope of bypassing the switch's functionality is through poisoning and flooding (discussed in subsequent chapters).

Sniffers operate at the OSI model's data link layer, which means they do not have to play by the same rules as the applications and services that reside further up the stack. Sniffers can capture everything on the wire and record it for later review. They allow the user's to see all of the data contained in the packet. While sniffers are still a powerful tool in an attacker's hands, they have lost some of their mystical statuses as many more people are using encryption.

Question 28:
NIST defines risk management as the process of identifying, assessing, and controlling threats to an organization's capital and earnings. But what is the "risk" itself?

- **Potential that a threat will exploit vulnerabilities of an asset or group of assets.**
- **Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.**
- **The unauthorized disclosure, modification, or use of sensitive data.**
- **An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system.**

Explanation
https://csrc.nist.gov/glossary/term/risk
The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Question 29:
What Linux command will you use to resolve a domain name into an IP address?

- **host -t ns resolveddomain.com**
- **host -t a resolveddomain.com**
- **host -t AXFR resolveddomain.com**
- **host -t soa resolveddomain.com**

Explanation
https://www.cyberciti.biz/faq/unix-linux-dns-lookup-command/

Input:

$ host -t a resolveddomain.com

Sample output:

resolveddomain.com has address 75.126.153.206

Incorrect answers:

Input:

$ host -t a resolveddomain.com

Sample output:

resolveddomain.com name server ns2.nixcraft.net.

resolveddomain.com name server ns1.nixcraft.net.

resolveddomain.com name server ns5.nixcraft.net.

resolveddomain.com name server ns4.nixcraft.net.

Input:

$ host -t soa resolveddomain.com

Sample output:

resolveddomain.com has SOA record ns1.nixcraft.net. vivek.nixcraft.com. 2008072353 10800 3600 604800 3600

Question 30:
The attacker managed to gain access to Shellshock, and now he can execute arbitrary commands and gain unauthorized access to many Internet-facing services. Which of the following operating system can't be affected by an attacker yet?

- **Windows**
- **OS X**
- **Linux**
- **Unix**

Explanation
https://en.wikipedia.org/wiki/Shellshock_(software_bug)
Shellshock, also known as Bashdoor, is a family of security bugs in the Unix Bash shell, the first of which was disclosed on 24 September 2014. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access to many Internet-facing services, such as web servers, that use Bash to process requests.

The Shellshock bug affects Bash, a program that various Unix-based systems use to execute command lines and command scripts. It is often installed as the system's default command-line interface. Analysis of the source code history of Bash shows the bug was introduced on 5 August 1989, and released in Bash version 1.03 on 1 September 1989.

Shellshock is a privilege escalation vulnerability that offers a way for users of a system to execute commands that should be unavailable to them. This happens through Bash's "function export" feature, whereby command scripts created in one running instance of Bash can be shared with subordinate instances. This feature is implemented by encoding the scripts within a table that is shared between the instances, known as the environment variable list. Each new instance of Bash scans this table for encoded scripts, assembles each one into a command that defines that script in the new instance, and executes that command. The new instance assumes that the scripts found in the list come from another instance, but it cannot verify this, nor can it verify that the command that it has built is a properly formed script definition. Therefore, an attacker can execute arbitrary commands on the system or exploit other bugs that may exist in Bash's command interpreter, if the attacker has a way to manipulate the environment variable list and then cause Bash to run.

The presence of the bug was announced to the public on 2014-09-24, when Bash updates with the fix were ready for distribution, though it took some time for computers to be updated to close the potential security issue.

Question 31:
A digital signature is the digital equivalent of a handwritten signature or stamped seal. It is intended to solve the problem of tampering and impersonation in digital communications. Which of the following option does a digital signature NOT provide?

- **Integrity**
- **Non-repudiation**
- **Confidentiality**
- **Authentication**

Explanation
https://en.wikipedia.org/wiki/Digital_signature
Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent

by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret. Further, some non-repudiation schemes offer a timestamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Three main properties of a digital signature:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the identity of the source messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentication, non-repudiation, etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check; e.g., checking a certificate revocation list or via the Online Certificate Status Protocol. Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.

Question 32:
Lisandro is engaged in sending spam. To avoid blocking, he connects to incorrectly configured SMTP servers that allow e-mail relay without authentication (which allows Lisandro to fake information about the sender's identity). What is the name of such an SMTP server?

- **Weak SMTP.**
- **Message transfer agent.**
- **Open mail relay.**
- **Public SMTP server.**

Explanation
https://en.wikipedia.org/wiki/Open_mail_relay
An open mail relay is an SMTP server that is configured to allow anyone on the Internet to send email through it, not just mail destined to or originating from known users. Email relay or open mail relay used to be the default configuration in many mail servers; certainly, it was the way the Internet was at first set up. Still, now open mail relays have become unpopular because of their exploitation by spammers and frauds. Moreover, many relays have been closed or were placed on blacklists by other servers.

Many Internet service providers use Domain Name System-based Blackhole Lists (DNSBL) to disallow mail from open relays. Once a mail server is detected or reported that allows third parties to send mail through them, they will be added to one or more such lists, and other e-mail servers using those lists will reject any mail coming from those sites. The relay must not actually be used to send spam to be blacklisted; instead, it may be blacklisted after a simple test that confirms open access.

This trend reduced the percentage of mail senders that were open relays from over 90% down to well under 1% over several years. This led spammers to adopt other techniques, such as using botnets of zombie computers to send spam.

Question 33:
Identify which of the following will provide you with the most information about the system's security posture?

- **Phishing, spamming, sending trojans**
- **Wardriving, warchalking, social engineering**
- **Port scanning, banner grabbing, service identification**
- **Social engineering, company site browsing, tailgating**

Explanation
The most information about the system will be provided by:

· ***Port scanning*** is a method of determining which ports on a network are open and could be receiving or sending data**.**

· ***Banner Grabbing*** is a technique used to gain information about a computer system on a network and the services running on its open ports.

· ***Services Identification*** is to enumerate the services running on the TCP or UDP ports, as well as to identify the underlying operating system of the target.

Incorrect answers:

· ***Wardriving*** *i*s the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone.

· ***Warchalking*** *i*s the drawing of symbols in public places to advertise an open Wi-Fi network.

· ***Social engineering*** is the act of tricking someone into divulging information or taking action, usually through technology.

· ***Tailgating*****,** sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise. Tailgating provides a simple social engineering-based way around many security mechanisms one would think of as secure.

· ***Phishing*** is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.

· ***Spamming*** is the use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing).

Question 34:
Which mode of a NIC (interface) allows you to intercept and read each network packet that arrives in its entirety?

- **Simplex Mode**
- **Port forwarding**
- **Multicast**
- **Promiscuous mode**

Explanation
https://en.wikipedia.org/wiki/Promiscuous_mode
Promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is specifically programmed to receive. This mode is normally used for packet sniffing on a router or a computer connected to a wired network or one being part of a wireless LAN. Interfaces are placed into promiscuous mode by software bridges often used with hardware virtualization.

Incorrect answers:

Port forwarding https://en.wikipedia.org/wiki/Port_forwarding

Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network) by remapping the destination IP address and port number of the communication to an internal host.

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

Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

Simplex Mode https://en.wikipedia.org/wiki/Simplex_communication

The concept refers to the communication channel type in which the data can flow only in one direction, i.e., the communication is unidirectional.

Data Transmission mode defines the direction of the flow of information between two communication devices. This is not directly related to the topic of the exam and is added to confuse you.

Question 35:
When getting information about the web server, you should be familiar with methods GET, POST, HEAD, PUT, DELETE, TRACE. There are two critical methods in this list: PUT (upload a file to the server) and DELETE (delete a file from the server). When using nmap, you can detect all these methods. Which of the following nmap scripts will help you detect these methods?

- **http enum**
- **http-headers**
- **http ETag**
- **http-methods**

Explanation
https://www.tutorialspoint.com/http/http_methods.htm
The set of common methods for HTTP/1.1 is defined below and this set can be expanded based on requirements. These method names are case sensitive and they must be used in uppercase.

S.N.	Method and Description
1	**GET** The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
2	**HEAD** Same as GET, but transfers the status line and header section only.
3	**POST** A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
4	**PUT** Replaces all current representations of the target resource with the uploaded content.
5	**DELETE** Removes all current representations of the target resource given by a URI.
6	**CONNECT** Establishes a tunnel to the server identified by a given URI.
7	**OPTIONS** Describes the communication options for the target resource.
8	**TRACE** Performs a message loop-back test along the path to the target resource.

Incorrect answers:

http-enum https://nmap.org/nsedoc/scripts/http-enum.html

Enumerates directories used by popular web applications and servers.

This parses a fingerprint file that's similar in format to the Nikto Web application scanner. This script, however, takes it one step further by building in advanced pattern matching as well as having the ability to identify specific versions of Web applications.

You can also parse a Nikto-formatted database using http-fingerprints.nikto-db-path. This will try to parse most of the fingerprints defined in nikto's database in real time. More documentation about this in the nselib/data/http-fingerprints.lua file.

http-headers https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

HTTP header fields are components of the header section of request and response messages in the Hypertext Transfer Protocol (HTTP). They define the operating parameters of an HTTP transaction.

http ETag https://en.wikipedia.org/wiki/HTTP_ETag

The ETag or entity tag is part of HTTP, the protocol for the World Wide Web. It is one of several mechanisms that HTTP provides for Web cache validation, which allows a client to make conditional requests. This mechanism allows caches to be more efficient and saves bandwidth, as a Web server does not need to send a full response if the content has not changed. ETags can also be used for optimistic concurrency control to help prevent simultaneous updates of a resource from overwriting each other.

Question 36:
Identify an adaptive SQL Injection testing technique by the description:

A testing technique is used to discover coding errors by inputting massive amounts of random data and observing the changes in the output.

- **Fuzz Testing.**
- **Dynamic Testing.**
- **Functional Testing.**
- **Static application security testing.**

Explanation
https://en.wikipedia.org/wiki/Fuzzing
Fuzz testing is an automated or semi-automated testing technique which is widely used to discover defects which could not be identified by traditional functional testing methods. It involves providing invalid input data or massive random data (known as fuzz to the system) in order to test the system with an attempt to crash it or failing the built-in code of the software under test. If a vulnerability is detected, then fuzzer is a software tool which is used to identify potential causes. Fuzzers know to work the best for identifying vulnerabilities which are prone to be exploited by buffer overflow, DOS (Denial of Service), SQL injection and cross-site scripting.

Incorrect answers:

Functional Testing https://en.wikipedia.org/wiki/Functional_testing

Functional testing is a quality assurance (QA) process and a type of black-box testing that bases its test cases on the specifications of the software component under test. Functions are tested by feeding them input and examining the output, and internal program structure is rarely considered (unlike white-box testing). Functional testing is conducted to evaluate the compliance of a system or component with specified functional requirements. Functional testing usually describes what the system does.

Dynamic Testing https://en.wikipedia.org/wiki/Dynamic_testing

Dynamic testing (or dynamic analysis) is a term used in software engineering to describe the testing of the dynamic behavior of code. That is, dynamic analysis refers to the examination of the physical response from the system to variables that are not constant and change with time. In dynamic testing the software must actually be compiled and run. It involves working with the software, giving input values and checking if the output is as expected by executing specific test cases which can be done manually or with the use of an automated process. This is in contrast to static testing. Unit tests, integration tests, system tests and acceptance tests utilize dynamic testing. Usability tests involving a mock version made in paper or cardboard can be classified as static tests when taking into account that no program has been executed; or, as dynamic ones when considering the interaction between users and such mock version is effectively the most basic form of a prototype.

Static application security testing

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

Static application security testing (SAST) is used to secure software by reviewing the source code of the software to identify sources of vulnerabilities. Although the process of statically analyzing the source code has existed as long as computers have existed, the technique spread to security in the late 90s and the first public discussion of SQL injection in 1998 when Web applications integrated new technologies like JavaScript and Flash.

Unlike dynamic application security testing (DAST) tools for black-box testing of application functionality, SAST tools focus on the code content of the application, white-box testing. An SAST tool scans the source code of applications and its components to identify potential security vulnerabilities in their software and architecture. Static analysis tools can detect an estimated 50% of existing security vulnerabilities.

Question 37:
Which of the following is the type of message that sends the client to the server to begin a 3-way handshake while establishing a TCP connection?

- **SYN**
- **SYN-ACK**
- **ACK**
- **RST**

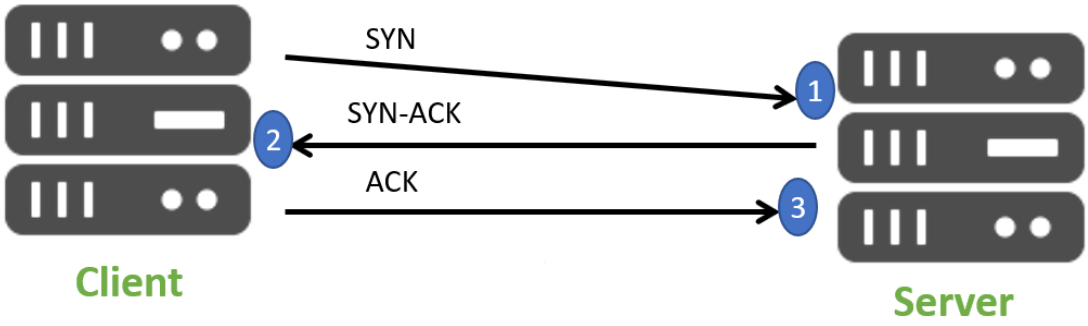
Explanation
https://en.wikipedia.org/wiki/Transmission_Control_Protocol#Connection_establishment
To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending an SYN to the server. The client sets the segment's sequence number to a random value A.

SYN-ACK: In response, the server replies with an SYN-ACK. The acknowledgement number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

At this point, both the client and server have received an acknowledgement of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, full-duplex communication is established.



Question 38:
Confidential information is stored and processed on your company's servers, however, auditing has never been enabled. What of the following should be done before enabling the audit feature?

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

Explanation
According to all kinds of specifications and recommendations, before introducing any new function (module, option, etc.) it's always necessary to first assess the risks and their impact on the end system.

Question 39:
Which of the following best describes of counter-based authentication system?

- **An authentication system that creates one-time passwords that are encrypted with secret keys.**
- **An authentication system that bases authentication decisions on behavioural attributes.**
- **An authentication system that bases authentication decisions on physical attributes.**
- **An authentication system that uses passphrases that are converted into virtual passwords.**

Explanation
In counter-based tokens, both the token and the authenticating server maintain a counter, whose value besides a shared secret key is used to generate the one-time password.

This type of token requires one or more actions from the user before generating and displaying the one-time password. Usually, the actions are pushing a power-on button, and in some types to enter a PIN number. The user action(s) will cause the token and the authenticating server to increment the counter.

Question 40:
Which of the following method of password cracking takes the most time?

- **Dictionary attack**
- **Brute force**
- **Rainbow tables**
- **Shoulder surfing**

Explanation
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 a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Such an attack might

be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

Brute-force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, the computational power required on average, to find the correct password increases exponentially.

Incorrect answers:

Rainbow tables 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.

Dictionary attack 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.

Shoulder surfing https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

A shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on a device or sensitive information being spoken and heard, also known as eavesdropping.

Question 41:
Leonardo, an employee of a cybersecurity firm, conducts an audit for a third-party company. First of all, he plans to run a scanning that looks for common misconfigurations and outdated software versions. Which of the following tools is most likely to be used by Leonardo?

- **Nmap**
- **Nikto**
- **Armitage**
- **Metasploit**

Explanation
https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)
Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

Incorrect answers:

Armitage https://en.wikipedia.org/wiki/Armitage_(computing)

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open-source network security tool notable for its contributions to red team collaboration allowing for: shared sessions, data, and communication through a single Metasploit instance.

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

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

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

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

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.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Question 42:
The absolute majority of routers and switches use packet filtering firewalls. That kind of firewalls makes decisions about allowing traffic to pass into the network based on the information contained in the packet header. At what level of the OSI model do these firewalls work?

- **Physical layer**
- **Session layer**
- **Application layer**
- **Network layer**

Explanation
https://en.wikipedia.org/wiki/Firewall_(computing)#Packet_filter
Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. Them make processing decisions based on network addresses, ports, or protocols. A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. If the packet passes the test, it's allowed to pass. If the packet doesn't pass, it's rejected.

Packet filters are the least expensive type of firewall. As a result, packet-filtering firewalls are very common. However, packet filtering has a number of flaws that knowledgeable hackers can exploit. As a result, packet filtering by itself doesn't make for a fully effective firewall.

One of the biggest weaknesses of packet filtering is that it pretty much trusts that the packets themselves are telling the truth when they say who they're from and who they're going to. Hackers exploit this weakness by using a hacking technique called IP spoofing, in which they insert fake IP addresses in packets that they send to your network.

Another weakness of packet filtering is that it examines each packet in isolation without considering what packets have gone through the firewall before and what packets may follow. In other words, packet filtering is stateless. Rest assured that hackers have figured out how to exploit the stateless nature of packet filtering to get through firewalls.

In spite of these weaknesses, packet filter firewalls have several advantages that explain why they are commonly used:

· *Packet filters are very efficient.* They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports are determined, the packet filter quickly applies its rules and either sends the packet along or rejects it. In contrast, other firewall techniques have a more noticeable performance overhead.

· *Packet filters are almost completely transparent to users*. The only time a user will be aware that a packet filter firewall is being used is when the firewall rejects packets. Other firewall techniques require that clients and/or servers be specially configured to work with the firewall.

· *Packet filters are inexpensive.* Most routers include built-in packet filtering.

Question 43:
Lisandro is a novice fraudster, he uses special software purchased in the depths of the network for sending his malware. This program allows it to deceive pattern-based detection mechanisms and even some behavior-based ones, disguising malwares as harmless programs. What does Lisandro use?

- **Crypter**
- **Ransomware**
- **Payload**
- **Dropper**

Explanation
A crypter is a type of software that can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. It is used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

Types of crypters

A crypter contains a crypter stub, or a code used to encrypt and decrypt malicious code. Depending on the type of stub they use, crypters can be classified as either static/statistical or polymorphic.

· Static/statistical crypters use different stubs to make each encrypted file unique. Having a separate stub for each client makes it easier for malicious actors to modify or, in hacking terms, "clean" a stub once it has been detected by a security software.

· Polymorphic crypters are considered more advanced. They use state-of-the-art algorithms that utilize random variables, data, keys, decoders, and so on. As such, one input source file never produces an output file that is identical to the output of another source file.

Incorrect answers:

Payload https://en.wikipedia.org/wiki/Payload_(computing)

In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message. Headers and metadata are sent only to enable payload delivery.

In the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action.

The term is borrowed from transportation, where payload refers to the part of the load that pays for transportation.

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

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion.

Dropper https://en.wikipedia.org/wiki/Dropper_(malware)

Droppers are programs that secretly install malicious programs, built into their code, on a computer. Typically, the programs dropped onto the victim's computer are saved and launched without any notification (or a fake notification may be displayed). Droppers are used to secretly install other malware or to help known malicious programs to evade detection (not all anti-malware programs are capable of scanning all components inside a dropper).

Question 44:
Enumeration is a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system. What type of enumeration is used to get shared resources on individual hosts on the network and a list of computers belonging to the domain?

- **Netbios enumeration**
- **SNMP enumeration**
- **NTP enumeration**
- **SMTP enumeration**

Explanation
https://en.wikipedia.org/wiki/NetBIOS
NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers.

NetBIOS names are used to identify network devices over TCP/IP (Windows). It must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers use the NetBIOS enumeration to obtain:

· List of computers that belong to a domain

· List of shares on the individual hosts on the network

· Policies and passwords

Incorrect answers:

SNMP enumeration https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs and switches other network devices on an IP network. SNMP is a very common protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers as well as network devices like routers, switches etc.

SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.

NTP enumeration https://en.wikipedia.org/wiki/Network_Time_Protocol

The Network Time Protocol is a protocol for synchronizing time across your network, this is especially important when utilizing Directory Services. There exists a number of time servers throughout the world that can be used to keep systems synced to each other. NTP utilizes UDP port 123. Through NTP enumeration you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client system in a network. All this information can be enumerated by querying NTP server.

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

The Simple Mail Transport Protocol is used to send email messages as opposed to POP3 or IMAP which can be used to both send and receive messages. SMTP relies on using Mail Exchange (MX) servers to direct the mail to via the Domain Name Service, however, should an MX server not be detected, SMTP will revert and try an A or alternatively SRV records. SMTP generally runs on port 25.

SMTP enumeration allows us to determine valid users on the SMTP server.

Question 45:
Having a sufficient database of passwords, you can use statistical analysis of the list of words, you can create a very effective way to crack passwords for such tools as, for example, John The Ripper. Which of the attacks uses such an analysis to calculate the probability of placing characters in a quasi-brute attack?

- **Prince**
- **Markov Chain**
- **Fingerprint**
- **Toggle-Case**

Explanation
Humans are considered the weakest link when it comes to data security since they will typically pick passwords that are easier to remember over something more secure. But this way, the password becomes easy to hack, as well. And even if the user has come up with a strong password, there are still numerous techniques to crack it open in just a few hours using a regular computer.

There are two main categories of password cracking techniques: offline and online.

· Online attacks are performed on a live host or system by either brute-force or wordlist attack against a login form, session, or another type of authentication technique.

· Offline attacks are made by extracting the password hash or hashes stored by the victim and attempting to crack them without alerting the targeted host, which makes offline attacks

the most widespread password cracking method. Security holes in the victim's infrastructure are what make this type of attack possible.

To use the Markov Chains technique, hackers need to assemble a certain password database, split each password into 2-grams and 3-grams (2- and 3-character-long syllables), and develop a new alphabet of different elements act as letters and then match it with the existing password database.

Finally, the hacker sets a threshold of occurrences that will be based on the next step and selects only the letters from the new alphabet that appear at least the minimum number of times, as chosen by the hacker. Then the method combines these into words of a maximum of eight characters in length and utilizes the dictionary attack once again.

Incorrect answers:

Toggle-Case

This attack creates every possible case combination for each word in a dictionary. The password candidate “do” would also generate “Do” and “dO.”

Fingerprint

This method is fairly sophisticated. It breaks possible passphrases down into “fingerprints,” single- and multi-character combinations that a user might choose. For the word “dog,” the technique would create fingerprints including “d,” “o,” “g,” along with “do,” and “og.”

This can be an especially effective attack when a user remembers part of a password. However, due to its sophistication, it requires extraordinary computing power.

Prince

Stands for “PRobability INfinite Chained Elements.” The PRINCE attack uses an algorithm to try the most likely password candidates with a refined combinator attack. It creates chains of combined words by using a single dictionary.

Question 46:
Alex, a network administrator, received a warning from IDS about a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. Now Alex needs to determine if these packets are genuinely malicious or simply a false positive. Which of the following type of network tools will he use?

- **Host-based intrusion prevention system (HIPS).**
- **Protocol analyzer.**
- **Vulnerability scanner.**
- **Intrusion Prevention System (IPS).**

Explanation
A network protocol analyzer is a tool used to monitor data traffic and analyze captured signals as they travel across communication channels. Sometimes network protocol analyzers are standalone hardware devices through which all network traffic is routed, and in other cases, they’re software applications installed on specific workstations or networks to provide an added layer of security. In addition, network protocol analyzers can be paired with firewalls and antivirus programs for a strong line of defense against network intrusions.

The most widely-used network protocol analyzer is Wireshark. For example, It can analyze information from PCAP files.

https://www.wireshark.org/

Incorrect answers:

Intrusion Prevention System (IPS)

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

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

Host-based intrusion prevention system (HIPS)

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

Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Vulnerability scanner https://en.wikipedia.org/wiki/Vulnerability_scanner

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans. Modern scanners are typically available as SaaS (Software as a service); provided over the internet and delivered as a web application. The modern vulnerability scanner often has the ability to customize vulnerability reports as well as the installed software, open ports, certificates and other host information that can be queried as part of its workflow.

Question 47:
Identify the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- **PKI**
- **single sign-on**
- **biometrics**
- **SOA**

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

Incorrect answers:

single sign-on https://en.wikipedia.org/wiki/Single_sign-on

Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

True single sign on allows the user to login once and access services without re-entering authentication factors.

It should not be confused with same-sign on (Directory Server Authentication), often accomplished by using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.

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

Biometric authentication refers to security processes that verify a user's identity through unique biological traits such as retinas, irises, voices, facial characteristics, and fingerprints.

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

Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. A SOA service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently, such as retrieving a credit card statement online. SOA is also intended to be independent of vendors, products and technologies.

Question 48:
Organizations need to deploy a web-based software package that requires three separate servers and internet access. What is the recommended architecture in terms of server placement?

- **A web server and the database server facing the Internet, an application server on the internal network.**
- **All three servers need to be placed internally.**
- **All three servers need to face the Internet so that they can communicate between themselves.**
- **A web server facing the Internet, an application server on the internal network, a database server on the internal network.**

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

In a three-tier application, all communication goes through the application tier. The presentation tier and the data tier cannot communicate directly with one another.

Presentation tier

The presentation tier is the user interface and communication layer of the application, where the end-user interacts with the application. Its main purpose is to display information to and collect information from the user. This top-level tier can run on a web browser, as a desktop application, or a graphical user interface (GUI), for example. Web presentation tiers are usually developed using HTML, CSS, and JavaScript. Desktop applications can be written in a variety of languages depending on the platform.

Application tier

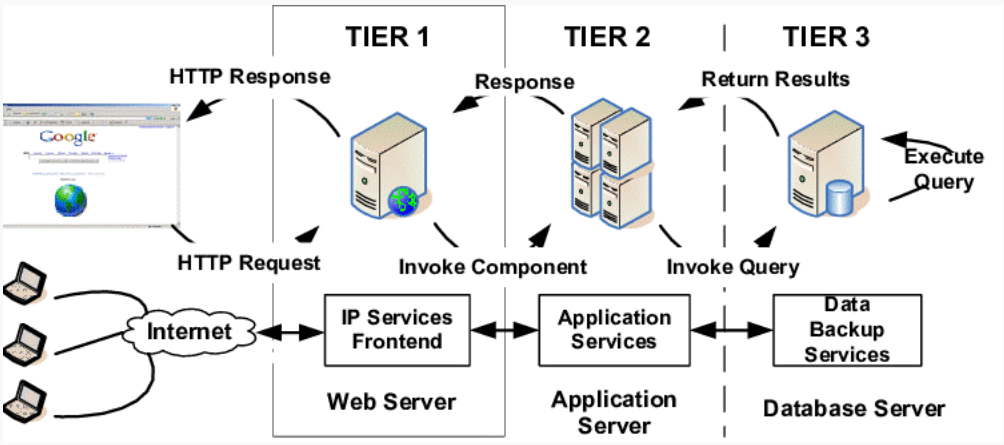
The application tier, also known as the logic tier or middle tier, is the heart of the application. In this tier, information collected in the presentation tier is processed - sometimes against

other information in the data tier - using business logic, a specific set of business rules. The application tier can also add, delete or modify data in the data tier.

The application tier is typically developed using Python, Java, Perl, PHP or Ruby, and communicates with the data tier using API calls.

Data-tier

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



Question 49:
Which of the following is true about the AES and RSA encryption algorithms?

- **AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.**
- **Both are asymmetric algorithms, but RSA uses 1024-bit keys.**
- **Both are symmetric algorithms, but AES uses 256-bit keys.**
- **RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data. (Correct)**

Explanation
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
The RSA algorithm is the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

RSA was first publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, though the 1973 creation of a public key algorithm by British mathematician Clifford Cocks was kept classified by the U.K.'s GCHQ until 1997.

Public key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys -- one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

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

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the [21st] century." It was intended to be easy to implement in hardware and software, as well as in restricted environments -- such as a smart card -- and offer decent defenses against various attack techniques.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.

Question 50:
Jack needs to analyze the files produced by several packet-capture programs such as Wireshark, tcpdump, EtherPeek and WinDump. Which of the following tools will Jack use?

- **tcptraceroute**
- **Nessus**
- **tcptrace**
- **OpenVAS**

Explanation
https://github.com/blitz/tcptrace
tcptrace is a TCP connection analysis tool. It can tell you detailed information about TCP connections by sifting through dump files. The dump file formats supported are:

· Standard tcpdump format (you need the pcap library)

· Sun's snoop format

· Macintosh Etherpeek format

· HP/NetMetrix protocol analysis format

· NS simulator output format

· NetScout

· NLANR Tsh Format

Incorrect answers:

tcptraceroute https://linux.die.net/man/1/tcptraceroute

tcptraceroute is a traceroute implementation using TCP packets.

The more traditional traceroute sends out either UDP or ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the

gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets are taking to reach the destination.

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

Nessus is a program for automatically searching for known flaws in the protection of information systems. It is able to detect the most common types of vulnerabilities, for example:

· Availability of vulnerable versions of services or domains

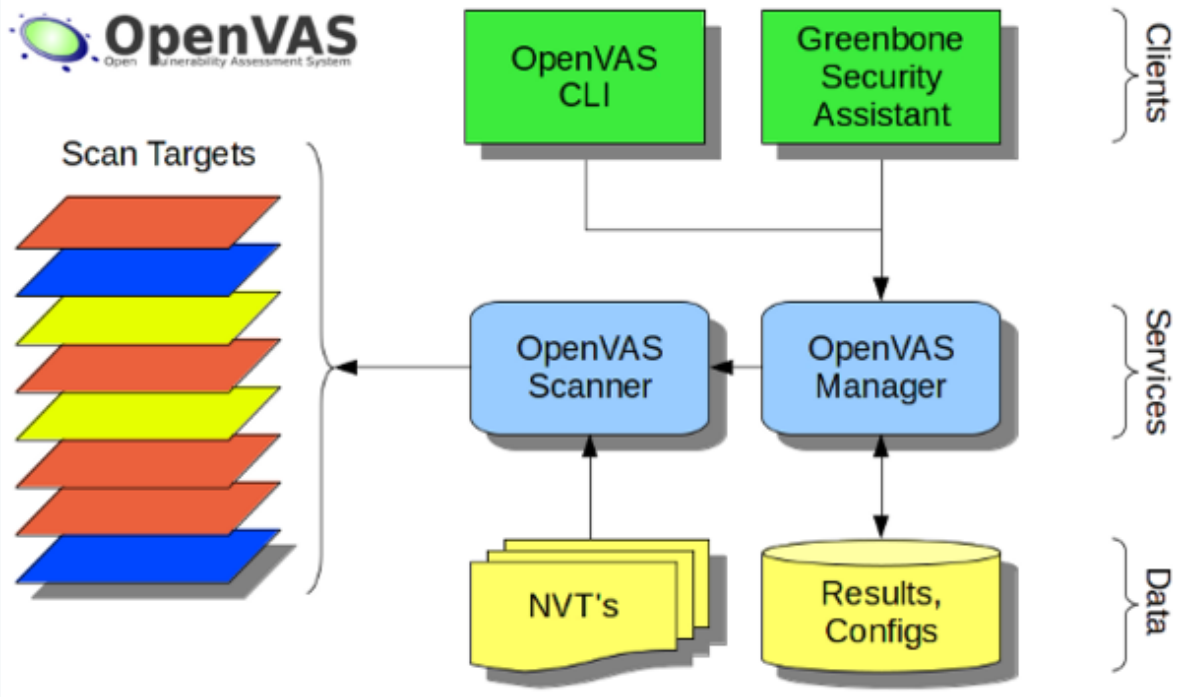
· Configuration errors (for example, no need for authorization on the SMTP server)

· Default, blank, or weak passwords

The program has a client-server architecture, which greatly expands the scanning capabilities. According to a survey conducted by securitylab.ru, 17% of respondents use Nessus.

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

OpenVAS (Open Vulnerability Assessment System, originally known as GNessUs) is a software framework of several services and tools offering vulnerability scanning and vulnerability management.



Question 51:
Which of the following nmap options can be used for very fast scanning?

- **-T0**
- **-O**
- **-T4**
- **-T5**

Explanation
If you don't worry about being detected and wanted to perform a very fast scan you can use option -T5.

```
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
```

Question 52:
Identify a tool that can be used for passive OS fingerprinting?

- **ping**
- **tcpdump**
- **nmap**
- **tracert**

Explanation
http://www.ouah.org/incosfingerp.htm#:~:text=In%20this%20paper%2C%20we%20will%20look%20at%20packets%20captured%20by%20TCPDUMP.&text=All%20that%20is%20needed%20to,a%20response%20from%20that%20machine.
The passive operating system fingerprinting is a feature built into the tcpdump tools. By the link provided in the explanation, you can take a closer look at the process of taking OS fingerprinting.

Incorrect answers:

nmap, ping and tracert are issuing packets and may studying the response to guess the OS.

Question 53:
ISAPI filters is a powerful tool that is used to extend the functionality of IIS. However, improper use can cause huge harm. Why do EC-Council experts recommend that security analysts monitor the disabling of unused ISAPI filters?

- **To defend against wireless attacks**
- **To prevent memory leaks**
- **To defend against webserver attacks**
- **To prevent leaks of confidential data**

Explanation
The security analyst should disable unnecessary ISAPI filters for all of the above reasons. ISAPI filters can be used to essentially open technological gateways. Thus, they can be used to open items that have already been cued as "access denied" and allow hackers to enter into web spaces that are intended to be confidential.

Question 54:
Identify a low-tech way of gaining unauthorized access to information?

- **Scanning**
- **Eavesdropping**
- **Sniffing**
- **Social engineering**

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

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques. The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals, and technicians to go unnoticed as they steal company secrets.

Incorrect answers:

Sniffing https://en.wikipedia.org/wiki/Sniffing_attack

A sniffing attack or a sniffer attack is theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.

Scanning

Scanning attacks is scan devices in HIS to gather network information of these devices before launching sophisticated attacks to undermine HIS security. Commonly used scanning techniques to gather computer network information include IP address scanning, port scanning, and version scanning.

Eavesdropping https://en.wikipedia.org/wiki/Network_eavesdropping

Network eavesdropping is a method that retrieves user information through the internet. This attack happens on electronic devices like computers and smartphones. This network attack typically happens under the usage of unsecured networks, such as public wifi connections or shared electronic devices. Eavesdropping attacks through the network is considered one of the most urgent threats in industries that rely on collecting and storing data.

Question 55:
Which of the following services run on TCP port 123 by default?

- **Telnet**
- **DNS**
- **NTP**
- **POP3**

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

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP was designed by David L. Mills of the University of Delaware.

NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area

networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

The protocol is usually described in terms of a client-server model, but can as easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. **Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123**. They can also use broadcasting or multicasting, where clients passively listen to time updates after an initial round-trip calibrating exchange. NTP supplies a warning of any impending leap second adjustment, but no information about local time zones or daylight saving time is transmitted.

Incorrect answers:

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

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a **connection to Transmission Control Protocol (TCP) port number 23**, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

POP3 https://en.wikipedia.org/wiki/Post_Office_Protocol

A POP3 server listens on well-known **port number 110** for service requests. Encrypted communication for POP3 is either requested after protocol initiation, using the STLS command, if supported, or by POP3S, which connects to the server using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) on well-known TCP **port number 995**.

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

DNS primarily uses the User Datagram Protocol (UDP) on **port number 53** to serve requests.

Question 56:
The SOC analyst of the company wants to track the transfer of files over the unencrypted FTP protocol, which filter for the Wireshark sniffer should he use?

- **tcp.port == 443**
- **tcp.port == 80**
- **tcp.port = 23**
- **tcp.port ==21**

Explanation
The question is simply on knowing the port number.

21 - File Transfer Protocol (FTP)

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

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.

Incorrect answers:

23 - teletype network (Telnet) https://en.wikipedia.org/wiki/Telnet

80 - HyperText Transfer Protocol (HTTP)

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

443 - HyperText Transfer Protocol Secure (HTTPS)

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

Question 57:
Your company regularly conducts backups of critical servers but cannot afford them to be sent off-site vendors for long-term storage and archiving. The company found a temporary solution in the form of storing backups in the company's safe. During the next audit, there was a risk associated with the fact that backup storages are not stored off-site. The company manager has a plan to take the backup storages home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- **Degauss the backup tapes and transport them in a lockbox.**
- **Encrypt the backup tapes and transport them in a lockbox.**
- **Encrypt the backup tapes and use a courier to transport them.**
- **Hash the backup tapes and transport them in a lockbox.**

Explanation
This is a very strange question, but, nevertheless, you can meet a similar question on the exam.

Firstly, it is not clear why The Manager of Information Technology takes backups home, as this contradicts all safety standards in companies.

Secondly, I will explain the logic behind the answer to this question by the method of exclusion:

Degauss the backup tapes and transport them in a lockbox, it's incorrect because degauss the backup tapes will result in data loss.

Hash the backup tapes and transport them in a lockbox, it's incorrect because the hash is a one-way function, and data on the backup tapes will be useless.

We only have 2 options left: "**Encrypt the backup tapes and transport them in a lockbox**" and "**Encrypt the backup tapes and use a courier to transport them**". Of course, we will choose the option with lockbox as this adds an extra layer of security.

Question 58:
Gabriella uses Google search operators, which allow you to optimize and expand the capabilities of regular search. What will be the result of this request?

site:eccouncil.org discount -ilearn

- **The results that match the entire query.**
- **Results about all discounts from the site eccouncil.org except for the ilearn format.**
- **Results about all discounts from the site ec-council.org for the ilearn training format.**
- **Results from the ec-council website except for discounts and the ilearn format.**

Explanation
https://moz.com/learn/seo/search-operators

- Put minus (-) in front of any term (including operators) to exclude that term from the results

- Put "site:" in front of a site or domain for search on a specific site

Well, you're right, this question is very easy and is a joke, but think about this. Google provides a whole ocean of information and the correct use of search tools will not only reduce your time that you spend on searches (for example, I spend a lot of it), but also make it more efficient. You can filter out ads, useless repetitions, pages that have not been updated for a long time, and so on. In the hands of a real researcher, this is a powerful tool for auditing. Google search operators are the basis of a hacker method that will allow you, for example, to find holes in the configuration and computer code that the website uses.

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

Question 59:
There are different ways of pentest of a system, network, or application in information security based on how much information you have about the target. There's black box testing, white box testing, and gray box testing. Which of the statements is true about grey-box testing?

- **The tester has full access to the internal structure.**
- **The tester is unaware of the internal structure.**
- **The tester does not have access at all.**
- **The tester only partially knows the internal structure.**

Explanation
https://en.wikipedia.org/wiki/Gray_box_testing
Gray-box testing is a combination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications. Gray-box testers require both high-level and detailed documents describing the application, which they collect in order to define test cases.

Gray-box testing is beneficial because it takes the straightforward technique of black-box testing and combines it with the code-targeted systems in white-box testing.

Gray-box testing is based on requirement test case generation because it presents all the conditions before the program is tested by using the assertion method. A requirement specification language is used to make it easy to understand the requirements and verify its correctness.

Question 60:
When choosing a biometric system for your company, you should take into account the factors of system performance and whether they are suitable for you or not. What determines such a factor as the throughput rate?

- **The probability that the system fails to detect a biometric input when presented correctly.**
- **The maximum number of sets of data that can be stored in the system.**
- **The data collection speeds, data processing speed, or enrolment time.**
- **The probability that the system incorrectly matches the input pattern to a non-matching template in the database.**

Explanation
https://www.ncsc.gov.uk/collection/biometrics/choosing-biometrics

The National Cyber Security Centre (NCSC) offers a list of questions and answers that you should go through, trying to decide which modality is suitable for your project(the full list is available at the link).

What are the locations and environments where biometric devices will be used?

Environmental factors, such as illumination, acoustic noise, and humidity, have consequences for each of the modalities. For example, face recognition is known to be more challenging in outdoor lighting conditions. Fingerprint systems struggle in high humidity or very dry conditions.

You will need to take into account any possible environmental factors which your proposed use will have to overcome.

Required throughput rate

Throughput can mean a number of different things - data collection speeds (e.g. the speed at which individuals can be processed at the data collection point), data processing speed or enrolment time.

For example, an access control system through a single portal taking 20 seconds to process each person would take nearly 2 hours to process a population of 300, most likely making the system unusable. Some modalities are inherently faster than others.

What is your target population?

Sensors will need to accommodate the range of people within a population, taking account of age, height, physical ability, ethnicity and other variations. The ergonomics of the biometric system must be designed with the target population in mind. Some biometric characteristics are harder to capture for some parts of a population. For example, fingerprint doesn't work as well with young children and older people as it does with those within the middle age ranges. The problem cases might not be obvious prior to deployment.

Question 61:
The attacker tries to find the servers of the attacked company. He uses the following command:

nmap 192.168.1.64/28

The scan was successful, but he didn't get any results.

Identify why the attacker could not find the server based on the following information:

The attacked company used network address 192.168.1.64 with mask 255.255.255.192. In the network, the servers are in the addresses192.168.1.122, 192.168.1.123 and 192.168.1.124.

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

Explanation
https://en.wikipedia.org/wiki/Subnetwork
The attacker uses a subnet mask / 28, the range of which is 15 IP addresses (0.0.0.15) and the range from 192.168.1.64 to 192.168.1.78 will be scanned.

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

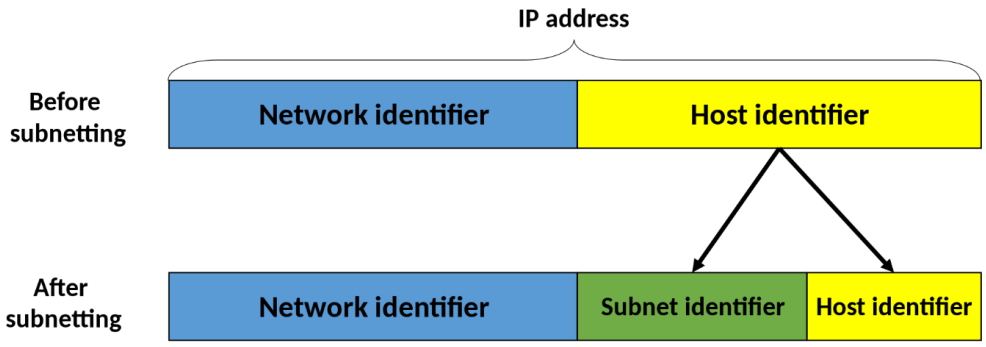
Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a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

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

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

Traffic is exchanged between subnetworks through routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between the subnets.

The benefits of subnetting an existing network vary with each deployment scenario. In the address allocation architecture of the Internet using CIDR and in large organizations, it is necessary to allocate address space efficiently. Subnetting may also enhance routing efficiency, or have advantages in network management when subnetworks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure, or other structures such as meshes.



CIDR	Last IP-адрес in Subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in a subnet
a.b.c.d/32	0.0.0.0	255.255.255.255	1	1*
a.b.c.d/31	0.0.0.1	255.255.255.254	2	2*
a.b.c.d/30	0.0.0.3	255.255.255.252	4	2
a.b.c.d/29	0.0.0.7	255.255.255.248	8	6
a.b.c.d/28	0.0.0.15	255.255.255.240	16	14
a.b.c.d/27	0.0.0.31	255.255.255.224	32	30
a.b.c.d/26	0.0.0.63	255.255.255.192	64	62
a.b.c.d/25	0.0.0.127	255.255.255.128	128	126
a.b.c.0/24	0.0.0.255	255.255.255.000	256	254
a.b.c.0/23	0.0.1.255	255.255.254.000	512	510

Question 62:
Victims of DoS attacks often are web servers of high-profile organizations such as banking, commerce, media companies, or government and trade organizations. Which of the following symptom could indicate a DoS or DDoS attack?

- **An inability to access any website**
- **Damage and corrupt files.**
- **Unknown programs running on your system.**
- **Misbehaviour of computer programs and application.**

Explanation

The theory behind a DDoS attack is simple, although attacks can range in their level of sophistication. Here's the basic idea. A DDoS is a cyberattack on a server, service, website, or network floods it with Internet traffic. If the traffic overwhelms the target, its server, service, website, or network is rendered inoperable.

DDoS attacks have definitive symptoms. The problem is, the symptoms are so much like other issues you might have with your computer — ranging from a virus to a slow Internet connection — that it can be hard to tell without a professional diagnosis. The symptoms of a DDoS include:

• Slow access to files, either locally or remotely

• A long-term inability to access a particular website

• Internet disconnection

• Problems accessing all websites

• Excessive amount of spam emails

Most of these symptoms can be hard to identify as being unusual. Even so, if two or more occur over long periods of time, you might be a victim of a DDoS.

Question 63:
Rajesh, a black-hat hacker, could not find vulnerabilities in the target company's network since their infrastructure is very well protected. IDS, firewall with strict rules, etc. He is trying to find such an attack method independent of the reliability of the infrastructure of this company. Which attack is an option suitable for Rajesh?

- **Buffer Overflow**
- **Denial-of-Service**
- **Social Engineering**
- **Confidence trick**

Explanation
https://en.wikipedia.org/wiki/Social_engineering_(security)
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

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

Incorrect answers:

Buffer Overflow https://en.wikipedia.org/wiki/Buffer_overflow

In information security and programming, 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 behaviour, including memory access errors, incorrect results, and crashes.

Exploiting the behaviour 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 behaviour that was not intended by the original programmer. Buffers are widespread in the 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.

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

In computing, 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.

Confidence trick https://en.wikipedia.org/wiki/Confidence_trick

A confidence trick is an attempt to defraud a person or group after first gaining their trust. Confidence tricks exploit victims using their credulity, naïveté, compassion, vanity, irresponsibility, and greed. Researchers have defined confidence tricks as "a distinctive species of fraudulent conduct ... intending to further voluntary exchanges that are not mutually beneficial", as they "benefit con operators ('con men') at the expense of their victims (the 'marks')."

Question 64:
Identify the attack where the hacker uses the ciphertexts corresponding to a set of plaintexts of his own choosing?

- **Kasiski examination**
- **Chosen-plaintext**
- **Differential cryptanalysis**
- **Known-plaintext attack**

Explanation
https://en.wikipedia.org/wiki/Chosen-plaintext_attack

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

Incorrect answers:

Differential cryptanalysis - is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key (cryptography key).

Known-plaintext attack - (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

Kasiski examination - (also referred to as Kasiski's test or Kasiski's method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenère cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846. In polyalphabetic substitution ciphers where the substitution alphabets are chosen by the use of a keyword, the Kasiski examination allows a cryptanalyst to deduce the length of the keyword. Once the length of the keyword is discovered, the cryptanalyst lines up the ciphertext in n columns, where n is the length of the keyword. Then each column can be treated as the ciphertext of a monoalphabetic substitution cipher. As such, each column can be attacked with frequency analysis.

Question 65:
Due to the network slowdown, the IT department decided to monitor the Internet traffic of all employees to track a possible cause, but they can't do it immediately. Which of the following is troublesome to take this kind of measure from a legal point of view?

- **The absence of an official responsible for traffic on the network.**
- **Not informing the employees that they are going to be monitored could be an invasion of privacy.**
- **Lack of comfortable working conditions.**
- **All of the employees would stop normal work activities.**

Explanation
Workplace monitoring is subject to various federal and state constitutional provisions and laws regarding when employees have a right to privacy and if and when they must be notified that they are being monitored. From a legal perspective, disclosing surveillance is the smartest tactic. Letting employees know that they will be monitored removes employees' reasonable expectation of privacy—the element that often forms the basis for invasion-of-privacy lawsuits arising under common law.

The two main restrictions on workplace monitoring are the Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. Section 2511 et seq.) and common-law protection against invasion of privacy. The ECPA is the only federal law that directly governs the monitoring of electronic communications in the workplace. Congress passed it in 1986 as an amendment to the federal Wiretap Act. Whereas the Wiretap Act restricted only the interception and monitoring of oral and wire communications, the ECPA extended those restrictions to electronic communications such as e-mail.

At first glance, the ECPA appears to prohibit an employer from intentionally intercepting its employees' oral, wire, and electronic communications. However, the ECPA contains several exceptions to this prohibition, and two of these exceptions are of particular importance to employers. The first is commonly known as the business purpose exception, which permits employers to monitor oral and electronic communications as long as the company can show a legitimate business purpose for doing so. The second is the consent exception, which allows employers to monitor employee communications provided that they have their

employees' consent to do so. An important and often overlooked distinction between the two exceptions is that the consent exception is not limited to business communications, and, therefore, a company arguably can monitor personal electronic communications if it can show employee consent. See May, an employee secretly record conversations with management and other employees without informing them?

In addition to these two exceptions, the ECPA contains a loophole that may limit employer liability for certain methods of monitoring. The act's definition of "electronic communications" expressly applies to the transmission of such communications and does not include such communications' electronic storage. Therefore, courts have distinguished between monitoring electronic communications such as e-mail messages while they are being transmitted versus viewing e-mails while they are in storage. Viewing stored e-mail is similar to searching through an employee's papers and files. Several courts confronting this issue have found that monitoring electronic communications after transmission does not run afoul of the ECPA.

The Stored Communications Act (SCA) is part of the ECPA and prohibits an entity providing an electronic communication service to the public from knowingly divulging electronic communication contents. It applies only to communications in which the employee had a reasonable expectation of privacy. When an employer makes it clear that certain communications are not protected, the SCA likely will not apply.

The ECPA merely sets the minimum restrictions on employee monitoring; individual states are free to impose greater limitations, and many have done so. For instance, in Connecticut, employers that monitor must provide employees advance written notice that specifies the specific types of monitoring methods. In addition, several state constitutions, including those of California, Florida, Louisiana, and South Carolina, expressly guarantee citizens a right to privacy. An explicit declaration of privacy in a state constitution may give employees heightened expectations of privacy, and employers in such states are wise to take additional steps to diminish employees' privacy expectations with respect to electronic information and communication in the workplace.

Question 66:
What is the name of the risk assessment method that allows you to study how various types of negative events (violations, failures or destructions) can affect the main activities of the company and key business processes?

- **Disaster Recovery Planning (DRP)**
- **Business Impact Analysis (BIA)**
- **Emergency Plan Response (EPR)**
- **Risk Mitigation**

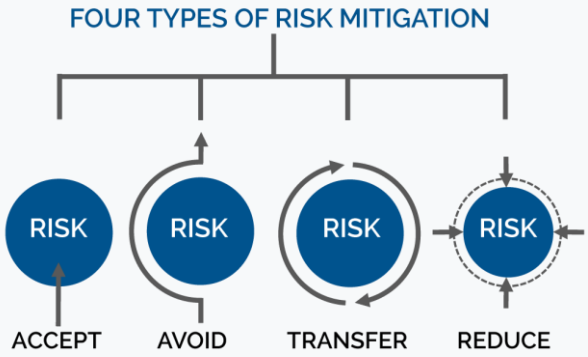
Explanation
Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations due to a disaster, accident, or emergency. A BIA is an essential component of an organization's business continuance plan. It includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied.

One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue normally if the cafeteria has to close but would come to a complete halt if the information system crashes. It is easy to confuse BIA and risk analysis, but they represent different steps in a business continuity plan.

Incorrect answers:

Risk Mitigation

Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.



Emergency Plan Response (EPR)

Emergency Response Plan — a set of written procedures for dealing with emergencies that minimize the impact of the event and facilitate recovery from the event.

Disaster Recovery Planning (DRP)

A disaster recovery plan (DRP) is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP). It is applied to the aspects of an organization that depend on a functioning IT infrastructure. A DRP aims to help an organization resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level.

Question 67:
Which of the following type of hackers refers to an individual who works both offensively and defensively?

- **White Hat**
- **Gray Hat**
- **Suicide Hacker**
- **Black Hat**

Explanation
https://en.wikipedia.org/wiki/Grey_hat
A grey hat (greyhat or gray hat) is a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards but does not have the malicious intent typical of a black hat hacker.

A further difference among these types of hackers lies in their methods of discovering vulnerabilities. The white hat breaks into systems and networks at the request of their employer or with explicit permission for the purpose of determining how secure it is against hackers, whereas the black hat will break into any system or network in order to uncover sensitive information for personal gain. The grey hat generally has the skills and intent of the white hat but will break into any system or network without permission.

According to one definition of a grey-hat hacker, when they discover a vulnerability, instead of telling the vendor how the exploit works, they may offer to repair it for a small fee. When one successfully gains illegal access to a system or network, they may suggest to the system administrator that one of their friends be hired to fix the problem; however, this practice has been declining due to the increasing willingness of businesses to prosecute. Another definition of Grey hat maintains that Grey hat hackers only arguably violate the law in an effort to research and improve security: legality being set according to the particular ramifications of any hacks they participate in.

Question 68:
While performing online banking using a browser, your friend receives a message that contains a link to a website. He decides to click on this link, and another browser session starts and displays a funny video. A few hours later, he receives a letter from the bank stating that his online bank was visited from another country and tried to transfer money. The bank also asks him to contact them and confirm the transfer if he really made it. What vulnerability did the attacker use when attacking your friend?

- **Cross-Site Request Forgery**
- **Webform input validation**
- **Cross-Site Scripting**
- **Clickjacking**

Explanation
https://en.wikipedia.org/wiki/Cross-site_request_forgery
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a 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, including inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Incorrect answers:

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.[1] 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.

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

Clickjacking (classified as a User Interface redress attack, UI redress attack, UI redressing) 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.

Webform input validation

Input validation attacks take place when an attacker purposefully enters information into a system or application with the intentions to break the system's functionality. Sometimes a web application can cause a malicious attack or input validation attack all while running in the background.

Question 69:
Which of the following is the most effective way against encryption ransomware?

- **Use multiple antivirus software.**
- **Pay a ransom.**
- **Analyze the ransomware to get the decryption key of encrypted data.**
- **Use the 3-2-1 backup rule.**

Explanation
https://en.wikipedia.org/wiki/Ransomware
The most effective way to handle ransomware attacks is to use the 3-2-1 backup rule: keep at least three separate versions of data on two different storage types with at least one offsite**.**

Question 70:
Which of the following modes of IPSec should you use to assure integrity and confidentiality of data within the same LAN?

- **ESP tunnel mode.**
- **AH tunnel mode.**
- **ESP transport mode.**
- **AH transport mode.**

Explanation
ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN.

Incorrect answers:

AH transport would only ensure the integrity of the LAN data, not the confidentiality; therefore, this answer is incorrect.

ESP tunnel mode should be used to secure the integrity and confidentiality of data between networks and not within a network; therefore, the answer is incorrect.

AH tunnel mode should be used to secure the integrity of data between networks and not within a network; therefore, the answer is incorrect.

Question 71:
To protect the enterprise infrastructure from the constant attacks of the evil hacker Ivan, Viktor divided the network into two parts using the network segmentation approach.

· In the first one (local, without direct Internet access), he isolated business-critical resources.

· In the second (external, with Internet access), he placed public web servers to provide services to clients.

Subnets communicate with each other through a gateway protected by a firewall. What is the name of the external subnet?

- **Demilitarized Zone**
- **WAF**
- **Bastion host**
- **Network access control**

Explanation
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.

The name is from the term demilitarized zone, an area between states in which military operations are not permitted.

Incorrect answers:

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

A bastion host is a server used to manage access to an internal or private network from an external network - sometimes called a jump box or jump server. Because bastion hosts often sit on the Internet, they typically run a minimum amount of services in order to reduce their attack surface. They are also commonly used to proxy and log communications, such as SSH sessions.

WAF https://en.wikipedia.org/wiki/Web_application_firewall

Web Application Firewall (WAF) helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks.

Network access control https://en.wikipedia.org/wiki/Network_Access_Control

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network. NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back-office servers and end-user computing equipment to ensure the information system is operating securely before interoperability is allowed. A basic form of NAC is the 802.1X standard.

Question 72:
After scanning the ports on the target machine, you see a list of open ports, which seems unusual to you:

```
1. Starting NMAP 5.21 at 2019-06-18 12:32
2. NMAP scan report for 172.19.40.112
3. Host is up (1.00s latency).
4. Not shown: 993 closed ports
```

```
PORT     STATE    SERVICE
21/tcp   open     ftp
23/tcp   open     telnet
80/tcp   open     http
139/tcp  open     netbios-ssn
515/tcp  open
631/tcp  open     ipp
9100/tcp open
MAC Address:  00:00:5D:3F:EE:92
```

Based on the NMAP output, identify what is most likely this host?

- **The host is likely a router.**
- **The host is likely a printer.**
- **The host is likely a Windows machine.**
- **The host is likely a Linux machine.**

Explanation

https://www.speedguide.net/port.php?port=515

You can see that port 515 is open from this we can conclude the host is likely a printer.

Port(s)	Protocol	Service	Details	Source
515	tcp	printer	Printing services, listening for incoming connections Trojans using this port: MscanWorm, lpdw0rm, Ramen. Multiple buffer overflows in Client Software WinCom LPD Total 3.0.2.623 and earlier allow remote attackers to execute arbitrary code via a long 0x02 command to the remote administration service on TCP port 13500 or a long invalid control filename to LPDService.exe on TCP port 515. References: [CVE-2008-5176], [BID-27614] Stack-based buffer overflow in Winlpd 1.26 allows remote attackers to execute arbitrary code via a long string in a request to TCP port 515. References: [CVE-2006-3670] [SECUNIA-21058] [BID-19011] [OSVDB-27332] Buffer overflow in NIPrint 4.10 allows remote attackers to execute arbitrary code via a long string to TCP port 515. References: [CVE-2003-1141] [BID-8968] [OSVDB-2774] [SECUNIA-10143] SAPlpd through 7400.3.11.33 in SAP GUI 7.40 on Windows has a Denial of Service vulnerability (service crash) with a long string to TCP port 515. References: [CVE-2016-10079], [EDB-41030] spooler (IANA official)	*SG*
515	tcp		Line Printer Daemon - print service (official)	*Wikipedia*
515	tcp	trojan	MscanWorm, Ramen	*Trojans*
515	tcp,udp	printer	spooler (lpd)	*Nmap*
515	tcp	lpdw0rm	[trojan] lpdw0rm	*Neophasis*
515	tcp	Ramen	[trojan] Ramen	*Neophasis*
515	tcp,udp	printer	spooler	*IANA*

Question 73:

John needs to send a super-secret message, and for this, he wants to use the technique of hiding a secret message within an ordinary message. The technique provides "security through obscurity." Which of the following techniques will John use?

- **Digital watermarking**
- **Encryption**
- **Steganography**
- **Deniable encryption**

Explanation

Steganography is the art of hiding a secret message in an ordinary object. The secret message and ordinary objects can be an image, text, audio, files, etc. A user can hide the secret in an ordinary-looking object using some tools and techniques, and the receiver can then use a similar technique to get the secret back.

Steganography is required to send the message without disclosing the presence of the message. This is how steganography differs from cryptography. Cryptography ensured that the message is encrypted, and this crypto message will not make any sense to the user without decryption. A malicious user can intercept this message and try to recover the message or the key used to encrypt the message using cryptographic attacks (Here's a resource that will navigate you through cybersecurity attacks). Steganography ensures that the object in which the message is hidden will not attract the hackers to try and get the message as there is no sign that there is something in the ordinary-looking object. Steganography provides security through obscurity. If no one can see it, no one can crack it.

Incorrect answers:

Digital watermarking https://en.wikipedia.org/wiki/Digital_watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Deniable encryption https://en.wikipedia.org/wiki/Deniable_encryption

Plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists.

The users may convincingly deny that a given piece of data is encrypted, or that they are able to decrypt a given piece of encrypted data, or that some specific encrypted data exists. Such denials may or may not be genuine. For example, it may be impossible to prove that the data is encrypted without the cooperation of the users. If the data is encrypted, the users genuinely may not be able to decrypt it. Deniable encryption serves to undermine an attacker's confidence either that data is encrypted, or that the person in possession of it can decrypt it and provide the associated plaintext.

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

Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

Question 74:
Identify the algorithm according to the following description:

That wireless security algorithm was rendered useless by capturing packets and discovering the passkey in seconds. This vulnerability was strongly affected to TJ Maxx company. This vulnerability led to a network invasion of the company and data theft through a technique known as wardriving.

- **Wi-Fi Protected Access (WPA)**
- **Wi-Fi Protected Access 2 (WPA2)**
- **Temporal Key Integrity Protocol (TKIP)**
- **Wired Equivalent Privacy (WEP)**

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

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not

necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

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

In 2007, the company disclosed a computer security breach dating back to 2005: computer hackers had gained access to information on credit and debit card accounts for transactions since January 2003. This exposed more than 100 million customers to potential theft from their accounts. According to the company, this affected customers who used their card between January 2003 and June 2004 at any branch of TJ Maxx. Details were stolen by hackers installing software via wi-fi in June 2005, that allowed them to access personal information on customers. The breach continued until January 2007.

In 2008 the Payment Card Industry (PCI) Security Standards Council updated the Data Security Standard (DSS) to prohibit use of WEP as part of any credit-card processing after 30 June 2010, and prohibit any new system from being installed that uses WEP after 31 March 2009.

Question 75:
What of the following is the most common method of using "ShellShock" or "Bash Bug"?

- **Using SSH.**
- **Through Web servers utilizing CGI to send a malformed environment variable.**
- **Manipulate format strings in text fields.**
- **Using SYN Flood.**

Explanation
The shellshock vulnerability arises from the underlying operating system using an older version of Bash in combination with a web server utilizing the common gateway interface (CGI) scripting language. An attacker can potentially use CGI to send a malformed environment variable to a vulnerable Web server and because the server uses Bash to interpret the variable, it will also run any malicious command tacked-on to it.

Question 76:
Which of the following is most useful for quickly checking for SQL injection vulnerability by sending a special character to web applications?

- **Semicolon**
- **Single quotation**
- **Double quotation**
- **Backslash**

Explanation
The best way to detect a SQL Injection vulnerability in a web application would be to put a single quote into a parameter in the application. Then, if they received an error, they could infer the presence of an SQL Injection vulnerability.

In a system (command interpreter, file system, or database management system, for example), characters that have special meanings are called metacharacters. For instance, in the SQL query context, single and double quotes are used as string delimiters. They are used both at the beginning and the end of a string. This is why when a single or double quote is injected into a query, the query breaks and throws an error.

The error returned due to the injection of a single quote may signify that the user's input was not filtered or sanitized in any way and that the input contains characters that have special meaning on the database.

Question 77:
John received this text message: "Hello, this is Jack Smith from the Gmail customer service. Kindly contact me about problems with your account: jacksmith@gmail.com". Which statement below is true?

- **John should write to jacksmith@gmail.com to verify the identity of Jack.**
- **This is a scam as everybody can get a @gmail.com address, not the Gmail customer service employees.**
- **This is a scam because John does not know Jack.**
- **This is probably a legitimate message as it comes from a respectable organization.**

Explanation
Anyone can register an email on yahoo, Gmail, etc. Scammers can easily use this to mislead the victim.

Question 78:
Which of the following stops vehicles from crashing through the doors of a building?

- **Bollards (Correct)**
- **Turnstile**
- **Mantrap**
- **Traffic barrier**

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

A bollard is a sturdy, short, vertical post. The term originally referred to a post on a ship or quay used principally for mooring boats but is now also used to refer to posts installed to control road traffic and posts designed to prevent ram-raiding and vehicle-ramming attacks.

Incorrect answers:

Mantrap https://en.wikipedia.org/wiki/Mantrap_(access_control)

A mantrap, air lock, sally port or access control vestibule is a physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. Airlocks have a very similar design, allowing free ingress and egress while also restricting airflow.

In a manual mantrap, a guard locks and unlocks each door in sequence. An intercom and/or video camera are often used to allow the guard to control the trap from a remote location.

In an automatic mantrap, identification may be required for each door, sometimes even possibly different measures for each door. For example, a key may open the first door, but a personal identification number entered on a number pad opens the second. Other methods of opening doors include proximity cards or biometric devices such as fingerprint readers or iris recognition scans.

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

A turnstile (also called a turnpike, baffle gate, automated gate in some regions) is a form of gate which allows one person to pass at a time. It can also be made so as to enforce one-way human traffic, and in addition, it can restrict passage only to people who insert a coin, a ticket, a pass, or similar. Thus a turnstile can be used in the case of paid access

(sometimes called a faregate or ticket barrier when used for this purpose), for example to access public transport, a pay toilet, or to restrict access to authorized people, for example in the lobby of an office building.

Traffic barrier https://en.wikipedia.org/wiki/Traffic_barrier

Traffic barriers (sometimes called Armco barriers, also known in North America as guardrails or guard rails and in Britain as crash barriers) keep vehicles within their roadway and prevent them from colliding with dangerous obstacles such as boulders, sign supports, trees, bridge abutments, buildings, walls, and large storm drains, or from traversing steep (non-recoverable) slopes or entering deep water. They are also installed within medians of divided highways to prevent errant vehicles from entering the opposing carriageway of traffic and help to reduce head-on collisions. Some of these barriers, designed to be struck from either side, are called median barriers. Traffic barriers can also protect vulnerable areas like schoolyards, pedestrian zones, and fuel tanks from errant vehicles.

Question 79:
Identify a security policy that defines using of a VPN for gaining access to an internal corporate network?

- **Information protection policy**
- **Access control policy**
- **Network security policy**
- **Remote access policy**

Explanation
https://en.wikipedia.org/wiki/Remote_access_policy
Remote access policy is a document which outlines and defines acceptable methods of remotely connecting to the internal network. It is essential in large organization where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks.

Incorrect answers:

Network security policy https://en.wikipedia.org/wiki/Network_security_policy

A network security policy is a formal document that outlines the principles, procedures and guidelines to enforce, manage, monitor and maintain security on a computer network. It is designed to ensure that the computer network is protected from any act or process that can breach its security.

Information protection policy

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

Information protection policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. Main goal is to ensure information is appropriately protected from modification or disclosure. It may be appropriate to have new employees sign policy as part of their initial orientation. It should define sensitivity levels of information.

Access control policy

Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, competence, authority, obligation, or conflict-of-interest factors. At a high level, access

control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. Access Control List is a familiar example.

Question 80:
Identify the type of DNS configuration in which first DNS server on the internal network and second DNS in DMZ?

- **Split DNS**
- **EDNS**
- **DynDNS**
- **DNSSEC**

Explanation
https://en.wikipedia.org/wiki/Split-horizon_DNS
split-horizon DNS (also known as split-view DNS, split-brain DNS, or split DNS) is the facility of a Domain Name System (DNS) implementation to provide different sets of DNS information, usually selected by the source address of the DNS request.

This facility can provide a mechanism for security and privacy management by logical or physical separation of DNS information for network-internal access (within an administrative domain, e.g., company) and access from an unsecure, public network (e.g. the Internet).

Implementation of split-horizon DNS can be accomplished with hardware-based separation or by software solutions. Hardware-based implementations run distinct DNS server devices for the desired access granularity within the networks involved. Software solutions use either multiple DNS server processes on the same hardware or special server software with the built-in capability of discriminating access to DNS zone records. The latter is a common feature of many server software implementations of the DNS protocol (cf. Comparison of DNS server software) and is sometimes the implied meaning of the term split-horizon DNS, since all other forms of implementation can be achieved with any DNS server software.

Incorrect answers:

DNSSEC https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

DynDNS https://en.wikipedia.org/wiki/Dynamic_DNS

Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses or other information.

EDNS https://en.wikipedia.org/wiki/Extension_Mechanisms_for_DNS

Extension Mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol. The first set of extensions was published in 1999 by the Internet Engineering Task Force as RFC 2671, also known as EDNS0 which was updated by RFC 6891 in 2013 changing the abbreviation slightly to EDNS(0).

Question 81:
Which of the following is an entity in a PKI that will vouch for the identity of an individual or company?

- **KDC**
- **CA**
- **CR**
- **VA**

Explanation
https://en.wikipedia.org/wiki/Certificate_authority
Certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third-party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

One particularly common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World Wide Web. Another common use is in issuing identity cards by national governments for use in electronically signing documents.

Incorrect answers:

KDC (key distribution center) https://en.wikipedia.org/wiki/Key_distribution_center

A key distribution center (KDC) is part of a cryptosystem intended to reduce the risks inherent in exchanging keys. KDCs often operate in systems within which some users may have permission to use certain services at some times and not at others.

For instance, an administrator may have established a policy that only certain users may back up to tape. Many operating systems can control access to the tape facility via a "system service". If that system service further restricts the tape drive to operate only on behalf of users who can submit a service-granting ticket when they wish to use it, there remains only the task of distributing such tickets to the appropriately permitted users. If the ticket consists of (or includes) a key, one can then term the mechanism which distributes it a KDC. Usually, in such situations, the KDC itself also operates as a system service.

CR (Certification Request)

CR (Certification Request) is the process of obtaining a certificate. Companies, through their RA (Registration Authority), or individuals, must request a digital certificate from a CA (Certification Authority). The request contains a public key and additional identity information. The CA will first investigate the validity of the request, and if successful will sign the public key, along with other variables presented by the party making the request. Once the certificate is signed, it may be used in the PKI (Public Key Infrastructure).

VA (Validation authority) https://en.wikipedia.org/wiki/Validation_authority

Validation authority (VA) is an entity that provides a service used to verify the validity of a digital certificate per the mechanisms described in the X.509 standard and RFC 5280

Question 82:
Alex, the system administrator, should check the firewall configuration. He knows that all traffic from workstations must pass through the firewall to access the bank's website. Alex

must ensure that workstations in network 10.10.10.0/24 can only reach the bank website 10.20.20.1 using HTTPS. Which of the following firewall rules best meets this requirement?

- **If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit**
- **If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit**
- **If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit**
- **If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit**

Explanation

Based on the data in the question, we understand that the source of the IP will be 10.10.10.0/24, which will connect to the IP 10.20.20.1, respectively, we add this information to the firewall rules.

We also see that the conditions indicate the connection via https:\\ (secure connection). All such secure transfers are done using port 443, the standard port for HTTPS traffic.

Based on the data above, the rule for the firewall should look like this: "If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit".

Question 83:

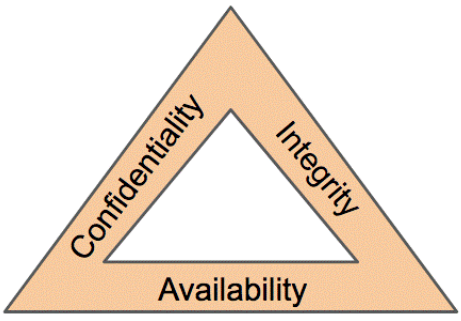
The CIA Triad is a security model that highlights the main goals of data security and serves as a guide for organizations to protect their confidential data from unauthorized access and data theft. What are the three concepts of the CIA triad?

- **Transference, transformation and transcendence**
- **Comparison, reflection and abstraction**
- **Efficiency, equity and liberty**
- **Confidentiality, integrity, and availability**

Explanation

https://en.wikipedia.org/wiki/Information_security#Key_concepts

The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. Every security control and every security vulnerability can be viewed in light of one or more of these key concepts. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA Triad.



Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." While similar to "privacy," the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

In information security, data integrity means maintaining and assuring data's accuracy and completeness over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases. However, it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity alongside confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Question 84:
Implementing the security testing process early in the SDLC is the key to finding out and fixing the security bugs early in the SDLC lifecycle. The security testing process can be performed in two ways, Automated or Manual web application security testing. Which of the proposed statements is true?

- **Automatic testing requires a lot of money and is still very imperfect, so it cannot be used for security**
- **Automatic and manual testing should be used together to better cover potential problems**
- **Manual testing is obsolete and should be completely replaced by automatic testing.**
- **Neural networks and artificial intelligence are already used in new tools and do not require additional actions**

Explanation
In using both automated and manual testing approaches, it is important to identify all possible attack surfaces, as a malicious attacker may only need one vulnerability to obtain unauthorized access to your sensitive information. Penetration testing companies often rely on a variety of automated and manual testing approaches, but it is best to understand each to achieve the greatest coverage.

Automated Tools

Speed: Automated tools work at a much faster rate by order of magnitude. It is much more difficult to manually test each component, service, and protocol manually with the same speed that a machine or script can.

Coverage: Capable of covering larger attack surfaces with more ease by implementing crawling of web applications to identify potential attack inputs especially “low hanging fruit” and technical related vulnerabilities. Manual testing would require a large amount of time

and skill to guarantee the same coverage and comparison to known vulnerabilities. Difficult for automated tools to accurately test in-house web applications and services which can result in missed logical vulnerabilities.

Efficiency: The processing capabilities of a machine are excellent. Automated tools can initialize and execute a large number of payloads for each test, but may not choose to execute the payloads correctly for each scenario. Usually, fuzz the application with multiple payloads and then wait for a reaction.

Qualifications: Automated tools have gone through intensive product testing for reliability and validity especially for professional versions. Manual testing skills is solely based on the individual pen tester's expert skillset and experience.

Reporting: Reports can be created easily and quickly. Usually, have graphical features such as charts for effective visual data comprehension. Can be generic output that may not be capable of describing how the finding was validated.

Investment: Open source tools and vulnerability scanners are usually free, but lack support or warranty. Professional licensing for vulnerability scanners and other automated tools can range dramatically in costs.

Manual Approach

Effectiveness: Automation alone is not capable to ensure that an application is thoroughly tested from a security perspective. Automated tools are poor at testing for logical vulnerabilities. Logical vulnerabilities require an understanding of the scope and flow of the application to identify any security issues. Certain findings, for example, CSRF (Cross-Site Request Forgery) and business logic vulnerabilities need an experienced certified security professional to be capable to exploit and validate all potential security scenarios.

Validity: Automated tool results usually contain a large number of false positives and negatives (30% to 90% depending on methodology and product) that can create a false sense of security or lack of security. These inaccuracies exist due to the lack of tool capabilities. It is the responsibility and expertise of the manual tester initializing the automated tool to validate the results and identify the true security findings.

Accuracy: Automated tools are only as reliable as their updates. If a new vulnerability or exploit has been introduced into the environment without a known category (i.e. zero-day), it is impossible for the automated tools to discover and identify the security threat. In manual testing, it is possible for the tester to create their own exploit depending on the situation and vulnerability. This allows the execution of comprehensive testing methodology that automated tools will overlook and fail to detect.

Custom Reporting: Once the penetration test is complete, the tester is capable of creating a comprehensive report that is as individual as the test results. At its most basic level, it will describe the vulnerabilities found, exploits used, data collected, risk rating, supportive evidence, affected assets, and mitigation recommendations. These reports are fine-tuned to the needs of the client so they gain the greatest security understanding of their infrastructure, application, or device.

Investment: The costs of manual testing depends on the scope and size of the engagement. In most penetration testing engagements, the cost and licensing of additional automated tools are covered under the negotiated penetration test contract unless special requirements call for installation of additional devices. In comparison, the cost of a data breach is growing exponentially as shown in current studies.

Question 85:
What type of cryptography is used in IKE, SSL, and PGP?

- **Public Key**
- **Hash**
- **Digest**
- **Secret Key**

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

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

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

PGP, SSL, and IKE use public-key cryptography.

Question 86:
The ping utility is used to check the integrity and quality of connections in networks. In the process, it sends an ICMP Echo-Request and captures the incoming ICMP Echo-Reply, but quite often remote nodes block or ignore ICMP. Which of the options will solve this problem?

- **Use arping**
- **Use traceroute**
- **Use hping**
- **Use broadcast ping**

Explanation
https://en.wikipedia.org/wiki/Hping
hping is an open-source packet generator and analyzer for the TCP/IP protocol created by Salvatore Sanfilippo. It is one of the common tools used for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique. The interface is inspired to the ping unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

Question 87:
An attacker tries to infect as many devices connected to the Internet with malware as possible to get the opportunity to use their computing power and functionality for automated attacks hidden from the owners of these devices. Which of the proposed approaches fits description of the attacker's actions?

- **Mass distribution of Ransomware**
- **APT attack**
- **Creating a botnet**
- **Using Banking Trojans**

Explanation
https://en.wikipedia.org/wiki/Botnet
A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software.

This example illustrates how a botnet is created and used for malicious gain:

· A hacker purchases or builds a Trojan and/or exploit kit and uses it to start infecting users' computers, whose payload is a malicious application—the bot.

· The bot instructs the infected PC to connect to a particular command-and-control (C&C) server. (This allows the botmaster to keep logs of how many bots are active and online.)

· The botmaster may then use the bots to gather keystrokes or use form grabbing to steal online credentials and may rent out the botnet as DDoS and/or spam as a service or sell the credentials online for a profit.

· Depending on the quality and capability of the bots, the value is increased or decreased.

Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. After the software is downloaded, it will call home (send a reconnection packet) to the host computer. When the re-connection is made, depending on how it is written, a Trojan may then delete itself or may remain present to update and maintain the modules.

Incorrect answers:

Using Banking Trojans https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

Banking trojans are a specific kind of trojan malware. Once installed onto a client machine, banking trojans use a variety of techniques to create botnets, steal credentials, inject malicious code into browsers, or steal money.

Mass distribution of Ransomware https://en.wikipedia.org/wiki/Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

APT attack https://en.wikipedia.org/wiki/Advanced_persistent_threat

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

Question 88:
To send an email using SMTP protocol which does not encrypt messages and leaving the information vulnerable to being read by an unauthorized person. To solve this problem, SMTP can upgrade a connection between two mail servers to use TLS, and the transmitted emails will be encrypted. Which of the following commands is used by SMTP to transmit email over TLS?

- **OPPORTUNISTICTLS**
- **UPGRADETLS**
- **STARTTLS**
- **FORCETLS**

Explanation
StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL. StartTLS is used with SMTP and IMAP, while POP3 uses a slightly different command for encryption, STLS.

The StartTLS process

SMTP always starts unencrypted. The StartTLS command starts the negotiation between server and client. Here's an outline of the communication that happens between the email client and the email server.

1. The process begins with the Transmission Control Protocol (TCP) handshake to help both the email client and server identify each other.

2. The server identifies with 220 Ready that the email client can proceed with the communication.

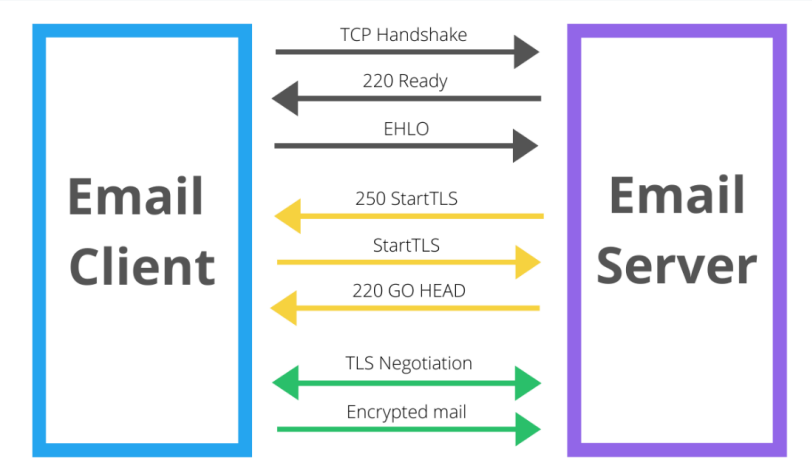
3. The client sends the server "EHLO" to inform the server that the client would like to use Extended SMTP (the more advanced version of SMTP that lets you include images, attachments, etc.).

4. The client sends "250-STARTTLS" to the mail server to ask whether or not StartTLS is accepted.

5. If the server sends back "go head," the StartTLS connection can be created.

6. The client restarts the connection and the email message has been encrypted.

NOTE:



Question 89:
The company secretly hired hacker Ivan to attack its competitors before a major tender. Ivan did not start with complex technological attacks but decided to hit the employees and their reputation. To do this, he collected personal information about key employees of a competitor company. Then he began to distribute it in the open form on the Internet by adding false information about past racist statements of employees. As a result of the scandal in social networks and the censure of employees, competitors lost the opportunity to win the tender, and Ivan's work was done. What is the name of this form of attack?

- **Vishing**
- **Piggybacking**
- **Doxing**
- **Daisy-chaining**

Explanation
https://en.wikipedia.org/wiki/Doxing
Doxing is the malicious identification and online publication of information about an individual. It can include Personally Identified Information (PII) or other sensitive, private, or damaging content about the individual's family members. Malicious actors dox victims in an attempt to harm them via the public exposure of their information.

Doxing is commonly retaliatory in nature (e.g., in reaction to controversial political opinions or actions). It may also be threatened as a means to extort victims, strategically compromise a person to influence their actions, or to affect public confidence in processes or systems. In some cases, doxing attacks contain concocted or factually inaccurate information designed to slander the victim, which sometimes mistakenly affects other victims with similar names, titles, or backgrounds.

Content posted on social media platforms and other publicly available information, such as home and work street addresses, email addresses, and telephone numbers, often acts as the foundation for doxing attacks. Though this information is publicly available, it can be used in aggregate with information from paid services or illicitly gathered information. Depending on the actor's skill and resources, doxes can contain information from compromises and data leaks, including financial or medical records, passwords, compromised account information, and email content.

The aggregation of information enables malicious actors to turn otherwise harmless content into a damaging collective. For example, separately, a person's last name, place of work, or home address is generally innocuous. However, when this information is combined, it could constitute PII and be weaponized against a target, especially if coupled with account information, passwords, and financial records.

Incorrect answers:

Daisy-chaining

It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.

Vishing https://en.wikipedia.org/wiki/Voice_phishing

Voice phishing, or vishing, is the use of telephony (often Voice over IP telephony) to conduct phishing attacks.

Piggybacking https://en.wikipedia.org/wiki/Piggybacking_(security)

Piggybacking, similar to tailgating, refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. It can be either electronic or physical. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.

Question 90:
Which of the following is a component of IPsec that performs protocol-level functions required to encrypt and decrypt the packets?

- **IPsec Policy Agent**
- **Internet Key Exchange (IKE)**
- **IPsec driver**
- **Oakley**

Explanation
This question is based on the information provided in the EC-Council's courseware:

IPsec driver: Software that performs protocol-level functions required to encrypt and decrypt packets.

Question 91:
You need to conduct a technical assessment of the network for a small company that supplies medical services. All computers in the company use Windows OS. What is the best approach for discovering vulnerabilities?

- **Check MITRE.org for the latest list of CVE findings.**
- **Use a scan tool like Nessus.**
- **Create a disk image of a clean Windows installation.**
- **Use the built-in Windows Update tool.**

Explanation
https://en.wikipedia.org/wiki/Nessus_(software)
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc.

Examples of vulnerabilities and exposures Nessus can scan for include:

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

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

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

· Denials of service vulnerabilities

· Nessus scans cover a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure.

Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system. Nessus can also support configuration and compliance audits, SCADA audits, and PCI compliance.

Incorrect answers:

Use the built-in Windows Update tool

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

Windows Update is a Microsoft service for the Windows 9x and Windows NT families of an operating system, which automates downloading and installing Microsoft Windows software updates over the Internet. The service delivers software updates for Windows, as well as the various Microsoft antivirus products, including Windows Defender and Microsoft Security Essentials. Since its inception, Microsoft has introduced two extensions of the service: Microsoft Update and Windows Update for Business. The former expands the core service to include other Microsoft products, such as Microsoft Office and Microsoft Expression Studio. The latter is available to business editions of Windows 10 and permits postponing updates or receiving updates only after they have undergone rigorous testing.

Check MITRE.org for the latest list of CVE findings

https://www.mitre.org/about/corporate-overview

https://cve.mitre.org/

As a not-for-profit organization, MITRE works in the public interest across federal, state and local governments, as well as industry and academia. We bring innovative ideas into existence in areas as varied as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

Question 92:
As a result of the attack on the dating web service, Ivan received a dump of all user passwords in a hashed form. Ivan recognized the hashing algorithm and started identifying passwords. What tool is he most likely going to use if the service used hashing without salt?

- **Brute force**
- **Rainbow table**
- **XSS**
- **Dictionary attacks**

Explanation
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.

Incorrect answer:

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 a combination 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 an essential derivation function. This is known as an exhaustive key search.

XSS 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 a 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.

Dictionary attacks 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.

Question 93:
Evil Russian hacker Ivan is attacking again! This time, he got a job in a large American company to steal commercial information for his customer to gain a competitive advantage in the market. In his attack, Ivan used all available means, especially blackmail, bribery, and technological surveillance. What is the name of such an attack?

- **Social Engineering**
- **Business Loss**
- **Information Leakage**
- **Corporate Espionage**

Explanation
https://en.wikipedia.org/wiki/Industrial_espionage
Corporate espionage — sometimes also called industrial espionage, economic espionage, or corporate spying — is the practice of using espionage techniques for commercial or financial purposes.

Several techniques that fall under the umbrella of corporate espionage:

· Trespassing onto a competitor's property or accessing their files without permission;

· Posing as a competitor's employee in order to learn company trade secrets or other confidential information;

· Wiretapping a competitor;

· Hacking into a competitor's computers;

· Attacking a competitor's website with malware;

But not all corporate espionage is so dramatic. Much of it can take the simple form of an insider transferring trade secrets from one company to another — a disgruntled employee, for instance, or an employee who has been hired away by a competitor and takes information with them that they shouldn't.

Then there's competitive intelligence— to put it in infosec terms, the white hat hacking of corporate espionage. Competitive intelligence companies say they're legal and above board and gather and analyze information that's largely public that will affect their clients' fortunes: mergers and acquisitions, new government regulations, chatter on blogs and social media, and so forth. They might research the background of a rival executive — not to dig up dirt, they say, but to try to understand their motivations and predict their behavior. That's the

theory, anyway, though sometimes, as we'll see, the line separating these operators from criminality can be thin.

Incorrect answers:

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

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

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

Information Leakage https://en.wikipedia.org/wiki/Information_leakage

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.

Business Loss

A business loss occurs when your business has more expenses than earnings during an accounting period. The loss means that you spent more than the amount of revenue you made. In the context of this question, this is just a tricky option.

Question 94:
John, a cybersecurity specialist, wants to perform a syn scan in his company's network. He has two machines. The first machine (192.168.0.98) has snort installed, and the second machine (192.168.0.151) has kiwi Syslog installed. When he started a syn scan in the network, he notices that kiwi Syslog is not receiving the alert message from snort. He decides to run Wireshark in the snort machine to check if the messages are going to the kiwi Syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi Syslog machine?

- **tcp.dstport==514 && ip.dst==192.168.0.0/16**
- **tcp.srcport==514 && ip.src==192.168.0.98**
- **tcp.srcport==514 && ip.src==192.168.151**
- **tcp.dstport==514 && ip.dst==192.168.0.151**

Explanation
https://wiki.wireshark.org/DisplayFilters
We must configure the destination port at the destination IP. The destination IP is 192.168.0.150, where the kiwi Syslog is installed.

Question 95:
Sniffing is a process of monitoring and capturing all data packets passing through a given network. An intruder can capture and analyze all network traffic by placing a packet sniffer on a network in promiscuous mode. Sniffing can be either Active or Passive in nature. How does passive sniffing work?

- **This is the process of sniffing through the router.**

- **This is the process of sniffing through the switch.**
- **This is the process of sniffing through the hub.**
- **This is the process of sniffing through the gateway.**

Explanation

Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

Active Sniffing

Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

Passive Sniffing

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

Question 96:
A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. They are classified according to the place of their injection.

What type of rootkit loads itself underneath the computer's operating system and can intercept hardware calls made by the original operating system.

- **Application rootkit**
- **Hypervisor (Virtualized) Rootkits**
- **Memory rootkit**
- **Kernel mode rootkits**

Explanation

https://en.wikipedia.org/wiki/Rootkit#Hypervisor_level

A hypervisor rootkit takes advantage of the hardware virtualization and is installed between the hardware and the kernel acting as the real hardware. Hence, it can intercept the communication/requests between the hardware and the host operating system. Common detection applications that run in user or kernel mode are not effective in this case as the kernel may not know whether it is executed on the legitimate hardware.

Incorrect answers:

Kernel mode rootkits https://en.wikipedia.org/wiki/Rootkit#Kernel_mode

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.

Application rootkit

Simple rootkits run in user-mode and are called user-mode rootkits. Such rootkits modify processes, network connections, files, events and system services. It is the only type of rootkit that could be detected by a common antivirus application.

Memory rootkit

This type of rootkit hides in the computer's RAM. These rootkits carry out harmful activities in the background and have a short lifespan. They only live in the computer's RAM and will disappear after the reboot system.

Question 97:
Which of the following is a common IDS evasion technique?

- **Unicode characters**
- **Spyware**
- **Port knocking**
- **Subnetting**

Explanation
Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.

Incorrect answers:

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

Spyware describes software with malicious behaviour that aims to gather information about a person or organization and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security. This behaviour may be present in malware as well as in legitimate software. Websites may also engage in spyware behaviours like web tracking. Hardware devices may also be affected. Spyware is frequently associated with advertising and involves many of the same issues. Because these behaviours are so common and can have non-harmful uses, providing a precise definition of spyware is a difficult task.

Port knocking https://en.wikipedia.org/wiki/Port_knocking

A port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s).

Subnetting https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

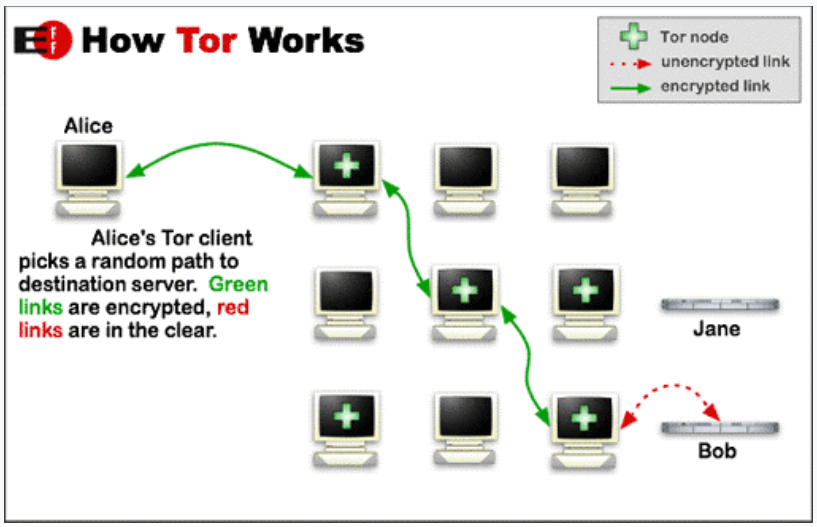
Question 98:
You want to surf safely and anonymously on the Internet. Which of the following options will be best for you?

- **Use Tor network with multi-node.**
- **Use VPN.**
- **Use public WiFi.**
- **Use SSL sites.**

Explanation
https://en.wikipedia.org/wiki/Tor_(anonymity_network)
Tor is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays in order to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored.

Tor does not prevent an online service from determining that it is being accessed through Tor. As a result, some websites restrict or even deny access through Tor. For example, Wikipedia blocks attempts by Tor users to edit articles unless special permission is sought.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication was partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination. An adversary may try to de-anonymize the user by some means. One way this may be achieved is by exploiting vulnerable software on the user's computer. The NSA had a technique that targets a vulnerability – which they codenamed "EgotisticalGiraffe" – in an outdated Firefox browser version at one time bundled with the Tor package and, in general, targets Tor users for close monitoring under its XKeyscore program. Attacks against Tor are an active area of academic research which is welcomed by the Tor Project itself.



Tor aims to conceal its users' identities and online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users anonymity in a network location. That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous onion service feature. Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.

Because the IP address of the sender and the recipient are not both in cleartext at any hop along the way, anyone eavesdropping at any point along the communication channel cannot directly identify both ends. Furthermore, to the recipient, it appears that the last Tor node (called the exit node), rather than the sender, is the originator of the communication.

Question 99:
How can resist an attack using rainbow tables?

- **Use of non-dictionary words.**
- **Use password salting.**
- **Lockout accounts under brute force password cracking attempts.**
- **All uppercase character passwords.**

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

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

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

Here is an incomplete example of a salt value for storing passwords. This first table has two username and password combinations. The password is not stored.

Username	Password
user1	password123
user2	password123

The salt value is generated at random and can be any length, in this case the salt value is 16 bytes long. The salt value is appended to the plaintext password and then the result is

hashed, this is referred to as the hashed value. Both the salt value and hashed value are stored.

Username	Salt value	String to be hashed	Hashed value = SHA256 (Password + Salt value)
user1	E1F53135E559C253	**password123**E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	84B03D034B409D4E	**password123**84B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

As the table above illustrates, different salt values will create completely different hashed values, even when the plaintext passwords are exactly the same. Additionally, dictionary attacks are mitigated to a degree as an attacker cannot practically precompute the hashes. However, a salt cannot protect common or easily guessed passwords.

Question 100:
Which of the following best describes the operation of the Address Resolution Protocol?

- **It sends a reply packet for a specific IP, asking for the MAC address.**
- **It sends a request packet to all the network elements, asking for the MAC address from a specific IP.**
- **It sends a request packet to all the network elements, asking for the domain name from a specific IP.**
- **It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.**

Explanation
https://en.wikipedia.org/wiki/Address_Resolution_Protocol
When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

All operating systems in an IPv4 Ethernet network keep an ARP cache. Whenever a host requests a MAC address to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not exist, then the request for network addresses is sent, and ARP is performed.

ARP broadcasts a request packet to all the LAN machines and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

Host machines that don't know their own IP address can use the Reverse ARP (RARP) protocol for discovery.

An ARP cache size is limited and is periodically cleansed of all entries to free up space; in fact, addresses tend to stay in the cache for only a few minutes. Frequent updates allow other devices in the network to see when a physical host changes their requested IP address. In the cleaning process, unused entries are deleted, and any unsuccessful attempts to communicate with computers that are not currently powered on.

Question 101:
During the security audit, Gabriella used Wget to read exposed information from a remote server and got this result:

```
Server: nginx/1.21.0
Date: Mon, 02 Aug 2021 13:29:13 EST
Content-Type: text/html
Content-Length: 5683
Last-Modified: Thu, 05 Jul 2021 17:44:09 EST
Connection: keep-alive
ETag: "5bb65169-1633"
Accept-Ranges: bytes
```

What is the name of this method of obtaining information?

- **Banner grabbing**
- **SQL injection**
- **XML External Entities (XXE)**
- **Cross-site scripting**

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

A banner screen is a configurable text “welcome” display from a network host system. The text generally provides system information, such as data about the operating system (OS) and service packs, software versions, and web services.

Unconfigured banners display default information and may also present login screens, which make them a target of hackers in attacks called banner grabbing.

Banner grabbing is the act of capturing the information provided by banners, configurable text-based welcome screens from network hosts that generally display system information. Banners are intended for network administration.

Banner grabbing is often used for white hat hacking endeavors like vulnerability analysis and penetration testing gray hat activities, and black hat hacking. Banner screens can be accessed through Telnet at the command prompt on the target system’s IP address. Other tools for banner grabbing include Nmap, Netcat, and SuperScan. A login screen, often associated with the banner, is intended for administrative use but can also provide access to a hacker. Meanwhile, the banner data can yield information about vulnerable software and services running on the host system.

For the sake of security, if banners are not a requirement of business or other software on a host system, the services that provide them may be disabled altogether. Banners can also be customized to present disinformation or even a warning message for hackers.

Incorrect answers:

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. Attackers may use a cross-site scripting vulnerability 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 until 2007. XSS effects vary in range from a petty nuisance to a significant security risk, depending on the sensitivity of the vulnerable site's data and the nature of any security mitigation implemented by the site's owner network.

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.

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.

XML External Entities (XXE)

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

An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

Question 102:
Which characteristic is most likely not to be used by companies in biometric control for use on the company's territory?

- **Iris patterns**
- **Fingerprints**
- **Height/Weight**
- **Voice**

Explanation
https://en.wikipedia.org/wiki/Biometrics
Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to typing rhythm, gait, keystroke, signature, behavioural profiling, and voice. Some researchers have coined the term behaviour metrics to describe the latter class of biometrics.

Indicators of weight and height are much more difficult to use. The weight, for example, can be easily changed.

Question 103:
Alex, a cybersecurity science student, needs to fill in the information into a secured PDF-file job application received from a prospective employer. He can't enter the information because all the fields are blocked. He doesn't want to request a new document that allows the forms to be completed and decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which attack is the student attempting?

- **Brute-force attack**

- **Dictionary-attack**
- **Man-in-the-middle attack**
- **Session hijacking**

Explanation

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

In cryptanalysis and computer security, 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.

Incorrect answers:

Man-in-the-Middle Attack https://en.wikipedia.org/wiki/Man-in-the-middle_attack

In cryptography and computer security, a man-in-the-middle is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Session Hijacking https://en.wikipedia.org/wiki/Session_hijacking

In computer science, session hijacking, sometimes also known as cookie hijacking, exploits a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. It refers to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers. The HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or access to the saved cookies on the victim's computer. After successfully stealing appropriate session cookies, an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet. Modern web browsers use cookie protection mechanisms to protect the web from being attacked.

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

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Question 104:

TLS, also known as SSL, is a protocol for encrypting communications over a network. Which of the following statements is correct?

- **SSL/TLS uses do not uses asymmetric or symmetric encryption.**
- **SSL/TLS uses only symmetric encryption.**
- **SSL/TLS uses only asymmetric encryption.**
- **SSL/TLS uses both asymmetric and symmetric encryption.**

Explanation

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

SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data-in-transit. Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.

Using symmetric and asymmetric cryptography SSL/TLS achieves an excellent balance between safety and speed.

Question 105:
Which of the following Linux-based tools will help you change any user's password or activate disabled accounts if you have physical access to a Windows 2008 R2 and an Ubuntu 9.10 Linux LiveCD?

- **CHNTPW**
- **Cain & Abel**
- **SET**
- **John the Ripper**

Explanation
https://en.wikipedia.org/wiki/Chntpw
chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where Windows stores password hashes.

There are two ways to use the program: via the standalone chntpw utility installed as a package available in most modern Linux distributions or via a bootable CD/USB image.

Incorrect answers:

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

John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker.

Cain & Abel https://en.wikipedia.org/wiki/Cain_and_Abel_(software)

Cain and Abel (often abbreviated to Cain) is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

Question 106:
Ivan, a black-hat hacker, performs a man-in-the-middle attack. To do this, it uses a rogue wireless AP and embeds a malicious applet in all HTTP connections. When the victims went to any web page, the applet ran. Which of the following tools could Ivan probably use to inject HTML code?

- **Wireshark**
- **tcpdump**
- **Ettercap**
- **Aircrack-ng**

Explanation
https://en.wikipedia.org/wiki/Ettercap_(software)
The question states that the attacker used the man-in-the-middle attack (MITM) and the list contains only one tool that allows this type of attack - ettercap

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.

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. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

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

Aircrack-ng https://en.wikipedia.org/wiki/Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux, FreeBSD, macOS, OpenBSD, and Windows; the Linux version is packaged for OpenWrt and has also been ported to the Android, Zaurus PDA and Maemo platforms; and a proof of concept port has been made to the iPhone.

tcpdump https://en.wikipedia.org/wiki/Tcpdump

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

Tcpdump works on most Unix-like operating systems: Linux, Solaris, FreeBSD, DragonFly BSD, NetBSD, OpenBSD, OpenWrt, macOS, HP-UX 11i, and AIX. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows version of libpcap.

Question 107:
The evil hacker Ivan wants to attack the popular air ticket sales service. After careful study, he discovered that the web application is vulnerable to introduced malicious JavaScript code through the application form. This code does not cause any harm to the server itself, but when executed on the client's computer, it can steal his personal data. What kind of attack is Ivan preparing to use?

- **CSRF**
- **LDAP Injection**
- **XSS**
- **SQL injection**

Explanation
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 a 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.

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.

LDAP Injection https://en.wikipedia.org/wiki/LDAP_injection

LDAP injection is a code injection technique used to exploit web applications that could reveal sensitive user information or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores. LDAP injection exploits a security vulnerability in an application by manipulating input parameters passed to internal search, add or modify functions. When an application fails to properly sanitize user input, it is possible for an attacker to modify an LDAP statement.

CSRF https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery (CSRF), 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.

Question 108:
What is the first and most important phase that is the starting point for penetration testing in the work of an ethical hacker?

- **Gaining Access**
- **Scanning**
- **Maintaining Access**
- **Reconnaissance**

Explanation
In this stage, attackers act like detectives, gathering information to understand their target truly. From examining email lists to open source information, their goal is to know the network better than those who run and maintain it. They hone in on the technology's security aspect, study the weaknesses, and use any vulnerability to their advantage.

The reconnaissance stage can be viewed as the most important because it takes patience and time, from weeks to several months. Any information the infiltrator can gather on the company, such as employee names, phone numbers, and email addresses, will be vital.

Attackers will also start to poke the network to analyze what systems and hosts are there. They will note any changes in the system that can be used as an entrance point. For

example, leaving your network open for a vendor to fix an issue can also allow the cybercriminal to plant himself inside.

By the end of this pre-attack phase, attackers will have created a detailed map of the network, highlighted the system's weaknesses, and continued with their mission. Another point of focus during the reconnaissance stage is understanding the network's trust boundaries. With an increase in employees working from home or using their personal devices for work, there is an increase in data breaches.

Incorrect answers:

Scanning

Security scanning can mean many different things, but it can be described as scanning a website's security, web-based program, network, or file system for either vulnerabilities or unwanted file changes. The type of security scanning required for a particular system depends on what that system is used. The more complicated and intricate the system or network is, the more in-depth the security scan has. Security scanning can be done as a one-time check, but most companies who incorporate this into their security practices buy a service that continually scans their systems and networks.

Gaining Access

Though Information Gathering, scanning, and enumeration phases are crucial in any pen test, the ultimate goal of an attacker or pentester spending time in those early phases is to reach the Gaining Access phase. Gaining Access is the phase where an attacker obtains control over the target. Be it a network or a web application, "Gaining Access" is only the beginning. Maintaining Access and post-exploitation (elevating access and pivoting) are usually performed for lateral movement.

Maintaining Access

"Maintaining Access" is a phase of the pentest cycle that has a very concrete purpose – to allow the pentester to linger in the targeted systems until he acquires what information he considers to be valuable and then manages to extract it successfully from the system. However, as is often the case, it is easier said than done. Let's compare it to being in someone else's house without his permission – it is one thing to enter his home and walk around for a while, but it is another matter when you want to settle in for a little longer without attracting the owner's attention.

Question 109:
Identify the attack by the description:

It is the wireless version of the phishing scam. This is an attack-type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises but has been set up to eavesdrop on wireless communications.

When performing this attack, an attacker fools wireless users into connecting a device to a tainted hotspot by posing as a legitimate provider.

This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent website and luring people there.

- **Signal Jamming**

- **Sinkhole**
- **Evil Twin**
- **Collision**

Explanation

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

An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. The evil twin is the wireless LAN equivalent of the phishing scam.

This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent website and luring people there.

The attacker snoops on Internet traffic using a bogus wireless access point. Unwitting web users may be invited to log into the attacker's server, prompting them to enter sensitive information such as usernames and passwords. Often, users are unaware they have been duped until well after the incident has occurred.

When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction since it is sent through their equipment. The attacker is also able to connect to other networks associated with the users' credentials.

Fake access points are set up by configuring a wireless card to act as an access point (known as HostAP). They are hard to trace since they can be shut off instantly. The counterfeit access point may be given the same SSID and BSSID as a nearby Wi-Fi network. The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection. It can simply say the system is temporarily unavailable after obtaining a username and password.

Incorrect answers:

Collision https://en.wikipedia.org/wiki/Collision_attack

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision. This is in contrast to a preimage attack where a specific target hash value is specified.

Sinkhole Attack

A sinkhole attack is a type of attack where a compromised node tries to attract network traffic by advertising its fake routing update. One of the impacts of the sinkhole attacks is that it can be used to launch other attacks like selective forwarding attacks, acknowledge spoofing attacks, and drops or altered routing information.

Signal Jamming Attack

A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio (SINR). SINR is the ratio of the signal power to the sum of the interference power from other interfering signals and noise power.

Question 110:
The company is trying to prevent the security breach by applying a security policy in which all Web browsers must automatically delete their HTTP browser cookies upon termination. Identify the security breach that the company is trying to prevent?

- **Attempts by attackers to access passwords stored on the employee's computer.**
- **Attempts by attackers to determine the employee's web browser usage patterns.**
- **Attempts by attackers to access the user and password information stored in the company's SQL database.**
- **Attempts by attackers to access websites that trust the Web browser user by stealing the employee's authentication credentials.**

Explanation

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

A session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). After successfully stealing appropriate session cookies an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet. Modern web browsers use cookie protection mechanisms to protect the web from being attacked.

Question 111:
Identify which term corresponds to the following description:

It is can potentially adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

- **Vulnerability**
- **Risk**
- **Attack**
- **Threat**

Explanation

If an asset is what you're trying to protect, then a threat is what you're trying to protect against. It is one of the most common terms that we come across on a daily basis. In cybersecurity, a threat is basically a hypothetical event that has the potential to cause some performing damage to an organisation's business and other processes.

Incorrect answers:

Attack https://en.wikipedia.org/wiki/Cyberattack

In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit

the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities.

Vulnerability

A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

Risk

Risk is a combination of the threat probability and the impact of a vulnerability. In other words, risk is the probability of a threat agent successfully exploiting a vulnerability, which can also be defined by the following formula:

· Risk = Threat Probability * Vulnerability Impact

Identifying all potential risks, analyzing their impact and evaluating appropriate response is called risk management. It is a never-ending process, which constantly evaluates newly found threats and vulnerabilities. Based on a chosen response, risks can be avoided, mitigated, accepted, or transferred to a third-party.

Question 112:
IPsec is a suite of protocols developed to ensure the integrity, confidentiality, and authentication of data communications over an IP network. Which protocol is NOT included in the IPsec suite?

- **Encapsulating Security Protocol (ESP)**
- **Media Access Control (MAC)**
- **Authentication Header (AH)**
- **Security Association (SA)**

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

The following protocols make up the IPsec suite:

· ***Authentication Header (AH)***

The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.

· ***Encapsulating Security Protocol (ESP)***

ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.

· ***Security Association (SA)***

SA refers to several protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

Finally, while the Internet Protocol (IP) is not part of the IPsec suite, IPsec runs directly on top of IP.

Question 113:
Which of the following is an attack where used precomputed tables of hashed passwords?

- **Dictionary Attack**
- **Hybrid Attack**
- **Rainbow Table Attack**
- **Brute Force Attack**

Explanation
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. The use of a key derivation that employs a salt makes this attack infeasible.

Philippe Oechslin invented rainbow tables as an application of an earlier, simpler algorithm by Martin Hellman.

Incorrect answers:

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

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

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

In cryptanalysis and computer security, 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.

Hybrid Attack

This is a cyberattack where the perpetrator blends two or more kinds of tools to carry out the assault. A typical hybrid attack is one that merges a dictionary attack and a brute-force attack. The former would contain a list of potentially known credential matches (wordlist). The latter would apply a brute-force attack upon each possible match.

Question 114:
In which phase of the ethical hacking process can Google hacking be used?

For example:

```
allintitle: root passwd
```

- **Reconnaissance**
- **Scanning and Enumeration**
- **Maintaining Access**
- **Gaining Access**

Explanation

First we need to understand what is an allintitle: in Google Search Operators

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

intitle:

Find pages with a certain word (or words) in the title. In our example, any results containing the word “apple” in the title tag will be returned.

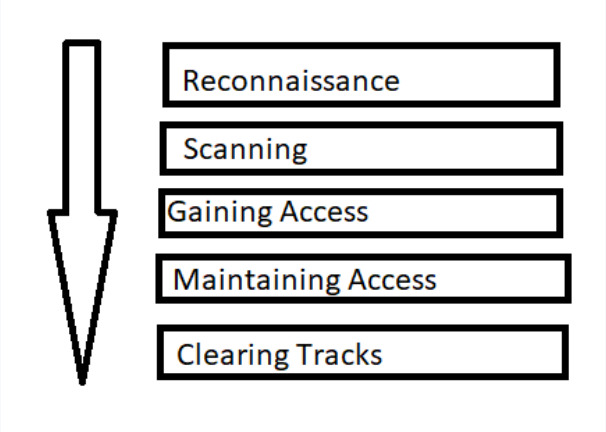
Example: intitle:apple

allintitle:

Similar to “intitle,” but only results containing all of the specified words in the title tag will be returned.

Example: allintitle:apple iphone

Based on the fact that we are just looking for information in the headings of web pages, we can confidently say that this belongs to the reconnaissance phase.



1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups:

· Network

· Host

· People involved

There are two types of Footprinting:

· *Active:* Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target

· *Passive:* Trying to collect information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

3. Gaining Access:

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain access to the target until he finishes the tasks he planned to accomplish in that target.

5. Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Question 115:
Black-hat hacker Ivan wants to determine the status of ports on a remote host. He wants to do this quickly but imperceptibly for IDS systems. For this, he uses a half-open scan that doesn't complete the TCP three-way handshake. What kind of scanning does Ivan use?

- **PSH Scan**
- **TCP SYN (Stealth) Scan**
- **XMAS scans**
- **FIN scan**

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

TCP SYN (Stealth) Scan (-sS)

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.

This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then

wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection (see https://nmap.org/misc/split-handshake.pdf).

Question 116:
Alex, an employee of a law firm, receives an email with an attachment "Court_Notice_09082020.zip". There is a file inside the archive "Court_Notice_09082020.zip.exe". Alex does not notice that this is an executable file and runs it. After that, a window appears with the notification "This word document is corrupt" and at the same time, malware copies data to APPDATA\local directory takes place in the background and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Alex encountered?

- **Trojan**
- **Worm**
- **Key-Logger**
- **Macro Virus**

Explanation
https://en.wikipedia.org/wiki/Trojan_horse_(computing)
A Trojan horse (or simply trojan) is any malware which 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. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. Ransomware attacks are often carried out using a trojan.

Unlike computer viruses, worms, and rogue security software, trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

Incorrect answers:

Worm 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 method to copy themselves without host program and distribute themselves based on the law of exponential growth, and then 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.

Macro Virus https://en.wikipedia.org/wiki/Macro_virus

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, Excel, PowerPoint allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected attachments in e-mails. Many antivirus programs can detect macro viruses; however, the macro virus' behavior can still be difficult to detect.

Key-Logger https://en.wikipedia.org/wiki/Keystroke_logging

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A keystroke recorder or keylogger can be either software or hardware.

While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, keyloggers are most often used for stealing passwords and other confidential information.

Keylogging can also be used to study keystroke dynamics or human-computer interaction. Numerous keylogging methods exist they range from hardware and software-based approaches to acoustic cryptanalysis.

Question 117:
What property is provided by using hash?

- **Integrity**
- **Confidentiality**
- **Authentication**
- **Availability**

Explanation
https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_messages_and_files
A cryptographic hash function (CHF) is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert

An important application of secure hashes is the verification of message integrity. Comparing message digests (hash digests over the message) calculated before, and after, transmission can determine whether any changes have been made to the message or file.

MD5, SHA-1, or SHA-2 hash digests are sometimes published on websites or forums to allow verification of integrity for downloaded files, including files retrieved using file sharing such as mirroring. This practise establishes a chain of trust as long as the hashes are posted on a trusted site - usually the originating site - authenticated by HTTPS. Using a cryptographic hash and a chain of trust detects malicious changes to the file. Other error detecting codes such as cyclic redundancy checks only prevent against non-malicious alterations of the file.

Incorrect answers:

Confidentiality

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Authentication

Authentication, in cryptography, can be used for authentication (and non-repudiation) services through digital signatures, digital certificates, or a Public Key Infrastructure (PKI).

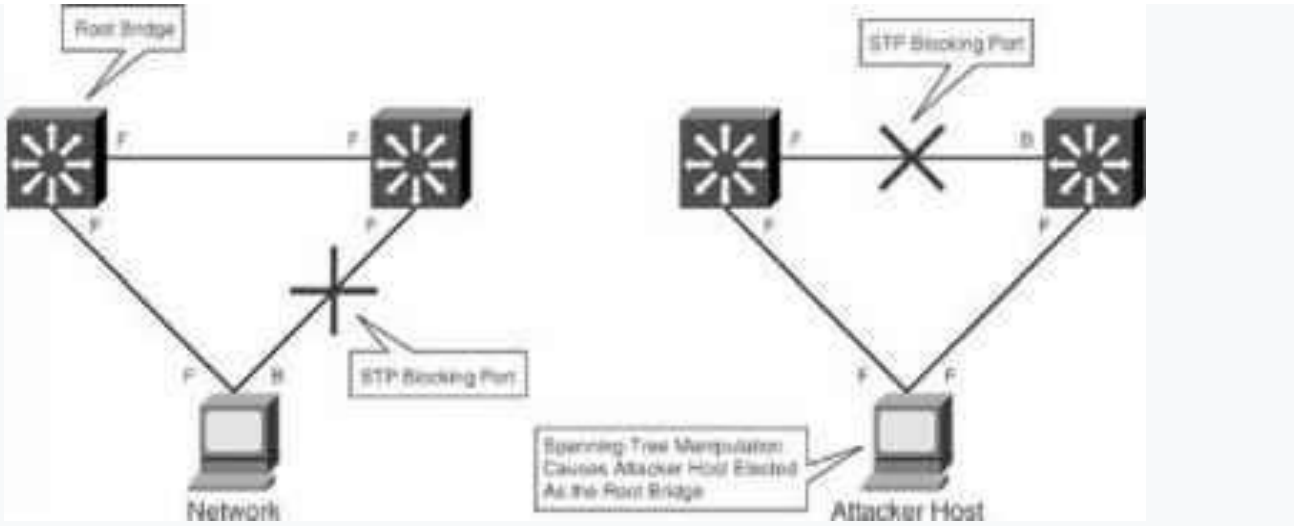
Question 118:
Assume an attacker gained access to the internal network of a small company and launches a successful STP manipulation attack. What are his next steps?

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

Explanation
STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.

STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgements (TCN/TCA) using bridge protocol data units (BPDU).

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. Figure 14-4 shows an attacker using STP network topology changes to force its host to be elected as the root bridge.



Question 119:
Monitoring your company's assets is one of the most important jobs you can perform. What warnings should you try to reduce when configuring security tools, such as security information and event management (SIEM) solutions or intrusion detection systems (IDS)?

- **Only True Negatives**
- **True Positives and True Negatives**
- **False Positives and False Negatives**
- **Only False Positives**

Explanation
The efficiency of any network security strategy depends on having accurate and complete visibility into what's going on. As part of this process, analysts need to investigate security alerts as these warning messages are, in theory, clear signs of a security incident. That's not always the case, though. On the one hand, many alerts are "false" in nature and burden security analysts with pointless investigations. On the other hand, some security incidents never generate an alert and fly under the radar. We need to defend against both situations if we want to prevent them from weakening our network security.

A false positive occurs when a security control identifies a file, network activity, website, or other activity as malicious – a positive detection – when it does not pose a threat. Hence, the term "false positive".

False negatives are a bigger concern than false positives because they result in real threats going undetected. Instead of receiving an alert for something that turns out to be a security issue, organizations receive no alert for something that does, in fact, pose a threat to their security. In other words, when something is analyzed, it's deemed not to be a threat – a negative assessment – and is released, even though it's malicious.

Question 120:
Jenny, a pentester, conducts events to detect viruses in systems. She uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which of the following methods does Jenny use?

- **Code Emulation.**
- **Integrity checking.**
- **Heuristic Analysis.**
- **Vulnerability scanner.**

Explanation
Code emulation is an extremely powerful virus detection technique. A virtual machine is implemented to simulate the CPU and memory management systems to mimic the code execution. Thus malicious code is simulated in the virtual machine of the scanner, and no actual virus code is executed by the real processor.

Incorrect answers:

Heuristic Analysis https://en.wikipedia.org/wiki/Heuristic_analysis

Heuristic analysis is a method employed by many computer antivirus programs designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".

Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs from statistical analysis, which bases itself on the available data/statistics.

Integrity checking

Integrity checking is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes.

Vulnerability scanner https://en.wikipedia.org/wiki/Vulnerability_scanner

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans.

Question 121:
Which of the following is an access control mechanism that allows multiple systems to use a CAS that permits users to authenticate once and gain access to multiple systems?

- **Single sign-on**
- **Discretionary Access Control (DAC)**
- **Role-Based Access Control (RBAC)**
- **Mandatory access control (MAC)**

Explanation
https://en.wikipedia.org/wiki/Single_sign-on
Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True single sign-on allows the user to login once and access services without re-entering authentication factors.

Incorrect answers:

Mandatory access control (MAC)

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

A security strategy that restricts individual resource owners' ability to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and cannot be altered by end-users.

Role-Based Access Control (RBAC)

https://en.wikipedia.org/wiki/Role-based_access_control

RBAC is a method of restricting network access based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Discretionary Access Control (DAC)

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

A discretionary access control (DAC) policy assigns access rights based on rules specified by users. The underlying philosophy in DAC is that subjects can determine who has access to their objects.

Question 122:
Identify the type of partial breaks in which the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key?

- **Information deduction.**
- **Global deduction.**
- **Instance deduction.**
- **Total break.**

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

Global deduction — the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

Incorrect answers:

Instance (local) deduction — the attacker discovers additional plaintexts (or ciphertexts) not previously known.

Information deduction — the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Total break — the attacker deduces the secret key.

Question 123:
Which of the following is a Denial-of-service vulnerability for which security patches have not yet been released, or there is no effective means of protection?

- **Zero-Day**
- **Smurf**
- **Yo-yo**
- **APDoS**

Explanation
Zero-days commonly refer to vulnerabilities in a system or application not previously known by the software vendor but known by attackers. Attackers can then possibly exploit the vulnerability to gain control of a system with relative ease since there aren’t any defenses in place. But what are "zero-day DDoS attacks," or so something like that even exists? To answer that, we need to look at what a “zero-day DDoS attack” would even mean.

In a sense, “zero-day DDoS attacks” do exist, but they’re not exactly zero-day. Periodically attackers will use a different protocol for their attack vector that hasn’t been used previously to launch a DDoS attack. This has happened quite a bit with reflection attacks where originally the attacks would use the DNS protocol, but over time reflection attacks have leveraged NTP, then SNMP, then SSDP, RIPv1, and even recently LDAP (or CLDAP). Thinking of these new attack vectors as zero-days gets a little hazy when considering that

these protocols have existed for many years. Additionally, attackers will perform some variation of an existing attack for a new or better effect.

In a sense, you can call the new attack vectors zero-days. DDoS mitigation vendors don't necessarily have custom signatures ready to detect these attacks automatically; they've had no time developing these signatures. However, these zero-days would not be limited to just different or new protocols being used — new botnets that use different source code to generate traffic and launch DDoS attacks also have their own unique signatures, even if they are using attacks that we've previously seen. Signatures for these botnets would need to be created to help aid in the automatic detection of an attack at any scale, and we would also need to analyze the sources of the traffic, which can help lead to the dismantling of the botnet.

Incorrect answers:

APDoS https://en.wikipedia.org/wiki/Denial-of-service_attack#Advanced_persistent_DoS

An advanced persistent DoS (APDoS) is associated with an advanced persistent threat and requires specialised DDoS mitigation. These attacks can persist for weeks; the longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

Smurf https://en.wikipedia.org/wiki/Smurf_attack

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

Yo-yo https://en.wikipedia.org/wiki/Denial-of-service_attack#Yo-yo_attack

A yo-yo attack is a specific type of DoS/DDoS aimed at cloud-hosted applications which use autoscaling. The attacker generates a flood of traffic until a cloud-hosted service scales outwards to handle the increase of traffic, then halts the attack, leaving the victim with over-provisioned resources. When the victim scales back down, the attack resumes, causing resources to scale back up again. This can result in a reduced quality of service during the periods of scaling up and down and a financial drain on resources during periods of over-provisioning, while operating with a lower cost for an attacker compared to a normal DDoS attack, as it only needs to be generating traffic for a portion of the attack period.

Question 124:
The fraudster Lisandro, masquerading as a large car manufacturing company recruiter, massively sends out job offers via e-mail with the promise of a good salary, a friendly team, unlimited coffee, and medical insurance. He attaches Microsoft Word or Excel documents to his letters into which he embeds a special virus written in Visual Basic that runs when the document is opened and infects the victim's computer. What type of virus does Lisandro use?

- **Polymorphic code**
- **Macro virus**
- **Stealth virus**
- **Multipart virus**

Explanation

https://en.wikipedia.org/wiki/Macro_virus
A macro virus is a virus written in a macro language: a programming language embedded inside a software application (e.g., word processors and spreadsheet applications). **Some applications, such as Microsoft Office, Excel, and PowerPoint, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened.** This provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected attachments in e-mails. Many antivirus programs can detect macro viruses; however, the macro virus' behaviour can still be difficult to detect.

Incorrect answers:

Polymorphic code https://en.wikipedia.org/wiki/Computer_virus#Polymorphic_code

Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus, therefore, has no parts which remain identical between infections, making it very difficult to detect directly using "signatures".[Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called "mutating engine" or "mutation engine") somewhere in its encrypted body. See polymorphic code for technical detail on how such engines operate.

Multipart virus

A multipartite virus is a computer virus that’s able to attack both the boot sector and executable files of an infected computer. Multipartite viruses are unique because of their ability to attack both the boot sector and executable files simultaneously, thereby allowing them to spread in multiple ways.

Stealth virus

A stealth virus is a virus that completely or partially hides its presence in the system by intercepting calls to the operating system that read, write, read additional information about infected objects (boot sectors, file system elements, memory, etc.)

Types of Stealth viruses:

· The boot virus intercepts the OS function intended for sector-by-sector access to disks in order to "show" the original contents of the sector to the user or the anti-virus program before infection.

· The file virus intercepts the functions of reading/setting position in a file, reading/writing to a file, reading a directory, etc. to hide the increase in the size of infected programs; intercepts the functions of reading/writing / displaying a file into memory to hide the fact that the file has changed.

· Macroviruses. It is quite simple to implement the stealth algorithm in macro viruses; you need to prohibit calling the File / Template or Tools / Macro menus; this can be achieved by deleting menu items from the list or replacing them with File Template and Tools Macro macros. Also, stealth viruses can be called macro viruses, which store their main code not in the macro itself but in other areas of the document.

Known Stealth viruses include viruses such as Virus.DOS.Stealth.551, Exploit.Macro.Stealth, Exploit.MSWord.Stealth, Brain, Fish # 6.

One of the first stealth viruses is considered to be RCE-04096, which was developed in Israel at the end of 1989. The name "Frodo" indicates the presence of the boot sector of the virus in its code, although it does not write its body to the boot sector.

Question 125:
What flags will be set when scanning when using the following command:

#nmap -sX host.companydomain.com

- **ACK flag is set.**
- **SYN flag is set.**
- **URG, PUSH and FIN are set.**
- **SYN and ACK flags are set.**

Explanation
https://nmap.org/book/scan-methods-null-fin-xmas-scan.html
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.