Question 1:
What is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication, authenticated denial of existence and data integrity, but not availability or confidentiality?

Zone transfer
Resource transfer
Resource records
DNSSEC

Explanation

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

Question 2:
Jack sent an email to Jenny with a business proposal. Jenny accepted it and fulfilled all her obligations. Jack suddenly refused his offer when everything was ready and said that he had never sent an email. Which of the following digital signature properties will help Jenny prove that Jack is lying?

Integrity
Non-Repudiation
Authentication
Confidentiality

Explanation

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

Incorrect answers:

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.

Authentication

Authentication is the process of verifying that the individual who sends a message is really who they say they are, and not an impostor.

Question 3:
Which of the following best describes a software firewall?
Software firewall is placed between the anti-virus application and the IDS components of the operating system.
Software firewall is placed between the desktop and the software components of the operating system.
Software firewall is placed between the router and the networking components of the operating system.
Software firewall is placed between the normal application and the networking components of the operating system.

Explanation
A software firewall is placed between the normal application and the networking components of the operating system and regulates data traffic through two things: port numbers, and applications. Depending on your firewall settings, your firewall could stop programs from accessing the Internet, and/or block incoming or outgoing access via ports.

For example, Port 80 is your Internet connection. Leaving outgoing Port 80 open is ok, because that is what allows you to browse the Internet. Leaving incoming Port 80 open is a different story. If it’s left open, anybody could access your network through Port 80.

One downside to a software-only firewall is that you have to train and maintain the software to recognize threats. As you add or update programs, your firewall will block them, until you tell it not to. Additionally it only protects the device it is installed on. That’s what it does by design**.**

Question 4:
What are the two main conditions for a digital signature?

- **Unique and have special characters.**
- **It has to be the same number of characters as a physical signature and must be unique.**
- **Unforgeable and authentic.**
- **Legible and neat.**

Explanation
This is a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are significant for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are several different encryption techniques to guarantee this level of security. The digital signature should also have the capability of being transported to other recipients. For instance, if a document is sent to a third party and they need to verify that the signature is authentic and if it is not readable on their software, it means that it will not be possible for them to access the document.

Question 5:
Maria is surfing the internet and try to find information about Super Security LLC. Which process is Maria doing?
Enumeration

System Hacking
Footprinting
Scanning

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

Footprinting is a part of the reconnaissance process used to gather possible information about a target computer system or network. It could be both passive and active. Reviewing a company’s website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information:

Domain name

IP Addresses

Namespaces

Employee information

Phone numbers

E-mails

Job Information

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.

One of the more popular open-source software platforms that run security scans is called Nmap. It has been around for a very long time and has the ability to find and exploit vulnerabilities in a network. Several online scans are available; however, these come with varying degrees of effectiveness and cost-efficiency.

NOTE: In the context of an EC-Council course and exam, think of these definitions like this:

Footprinting is a passive collection of information without touching the target system/network/computer.

Scanning is an active collection of information associated with a direct impact on the target.

Yes, that's not entirely true, but this course has big problems with abstraction levels. It is almost impossible to present a lot of topics in such a short period of time.

Enumeration

Enumeration is defined as a process that establishes an active connection to the target hosts to discover potential attack vectors in the system. The same can be used to exploit the system further. Enumeration is used to gather the below:

Usernames, Group names

Hostnames

Network shares and services

IP tables and routing tables

Service settings and Audit configurations

Application and banners

SNMP and DNS Details

System Hacking

System hacking is a vast subject that consists of hacking the different software-based technological systems such as laptops, desktops, etc. System hacking is defined as compromising computer systems and software to access the target computer and steal or misuse their sensitive information. Here, the malicious hacker exploits a computer system's weaknesses or network to gain unauthorized access to its data or take illegal advantage.

Question 6:
Maria conducted a successful attack and gained access to a Linux server. She wants to avoid that NIDS will not catch the succeeding outgoing traffic from this server in the future. Which of the following is the best way to avoid detection of NIDS?

- **Encryption.**
- **Out of band signaling.**
- **Alternate Data Streams.**
- **Protocol Isolation.**

Explanation
https://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today’s networks are primarily targeted against network services (application layer entities), the packet-level analysis ends up doing very little to protect our core business assets.

Question 7:
Ivan, a black hat hacker, sends partial HTTP requests to the target webserver to exhaust the target server’s maximum concurrent connection pool. He wants to ensure that all additional connection attempts are rejected. What type of attack does Ivan implement?

Fragmentation
Slowloris
Spoofed Session Flood
HTTP GET/POST

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

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

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

The program was named after Slow lorises, a group of primates that are known for their slow movement.

Incorrect answers:

HTTP GET/POST (HTTP Flood) https://en.wikipedia.org/wiki/HTTP_Flood

HTTP Flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker manipulates HTTP and POST unwanted requests in order to attack a web server or application. These attacks often use interconnected computers that have been taken over with the aid of malware such as Trojan Horses. Instead of using malformed packets, spoofing and reflection techniques, HTTP floods require less bandwidth to attack the targeted sites or servers.

Spoofed Session Flood

Fake Session attacks try to bypass security under the disguise of a valid TCP session by carrying an SYN, multiple ACK and one or more RST or FIN packets.

This attack can bypass defence mechanisms that are only monitoring incoming traffic on the network. These DDoS attacks can also exhaust the target’s resources and result in a complete system shutdown or unacceptable system performance.

Fragmentation https://en.wikipedia.org/wiki/IP_fragmentation_attack

IP fragmentation attacks are a kind of computer security attack based on how the Internet Protocol (IP) requires data to be transmitted and processed. Specifically, it invokes IP fragmentation, a process used to partition messages (the service data unit (SDU); typically a packet) from one layer of a network into multiple smaller payloads that can fit within the lower layer's protocol data unit (PDU). Every network link has a maximum size of messages that may be transmitted, called the maximum transmission unit (MTU). If the SDU plus metadata added at the link-layer exceeds the MTU, the SDU must be fragmented. IP fragmentation attacks exploit this process as an attack vector.

Part of the TCP/IP suite is the Internet Protocol (IP) which resides at the Internet Layer of this model. IP is responsible for the transmission of packets between network endpoints. IP includes some features which provide basic measures of fault-tolerance (time to live, checksum), traffic prioritization (a type of service) and support for the fragmentation of larger packets into multiple smaller packets (ID field, fragment offset). The support for fragmentation of larger packets provides a protocol allowing routers to fragment a packet into smaller packets when the original packet is too large for the supporting datalink frames. IP fragmentation exploits (attacks) use the fragmentation protocol within IP as an attack vector.

Question 8:
Define Metasploit module used to perform arbitrary, one-off actions such as port scanning, denial of service, SQL injection and fuzzing?

Payload Module.
NOPS Module.
Exploit Module.
Auxiliary Module.

Explanation
https://www.offensive-security.com/metasploit-unleashed/auxiliary-module-reference/

Auxiliary modules do not require the use of a payload to run like exploit modules. These types of modules include useful programs such as scanners, fuzzier, and SQL injection tools. Penetration testers use the plethora of scanners in the auxiliary directory to gather a deep understanding of the system to be attacked and then transition to exploit modules.

Incorrect answers:

Exploit Module

Exploit modules are pieces of code within the database that when running on a victim computer. The attacker will attempt to leverage a vulnerability on the local or remote system compromising the payload module such as the Meterpreter shell.

Payload Module

While using an exploit against a vulnerable machine, a payload is generally attached to the exploit before its execution. The payload contains the set of instructions that the victim’s computer is to carry out after compromise. Payloads come in many different flavors and can range from a few lines of code to small applications such as the Meterpreter shell. One should not just automatically jump to the Meterpreter shell. Metasploit contains over 200 different payloads

Bind Shells

These types of shell lay dormant and listen for an attacker to connect or send instructions. Bind shells are not a good choice for victim machines that are behind a firewall that does not have direct network access to the machine.

Reverse Shells

Reverse shells call home to the security tester for immediate instruction and interaction. If the compromised machine executes the exploit with a reverse payload, then a tester will be presented with a shell to access the machine and if they were sitting at the keyboard on the victim’s machine.

3. Meterpreter Shell

The Meterpreter shell, a special type of shell, is the bread and butter of Metasploit. The Meterpreter shell can be added as a payload that is either a bind shell or reverse shell.

NOPS Module

level language (assembly language), NOP is short for No Operation. This is most prevalently referred to for x86 chips as 0x90. At the point when a processor stacks that instruction, it basically does nothing (in any event helpful) for the one cycle and afterward progresses the register to the next instruction.

Question 9:
Which regulation defines security and privacy controls for all U.S. federal information systems except those related to national security?

PCI-DSS
NIST-800-53
EU Safe Harbor
HIPAA

Explanation
Correct answer: NIST-800-53

Explanation: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

https://nvd.nist.gov/800-53

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

Incorrect answers:

PCI-DSS https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

EU Safe Harbor

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

The International Safe Harbor Privacy Principles or Safe Harbour Privacy Principles were principles developed between 1998 and 2000 in order to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information.

HIPAA https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage

Question 10:
Ivan, a black hat hacker, tries to call numerous random numbers inside the company, claiming he is from the technical support service. It offers company employee services in exchange for confidential data or login credentials. What method of social engineering does Ivan use?

Reverse Social Engineering
Tailgating
Quid Pro Quo
Elicitation

Explanation
There is a social engineering technique "baiting" that exploits the human’s curiosity. Baiting is sometimes confused with other social engineering attacks. Its main characteristic is the promise of goods that hackers use to deceive the victims.

A classic example is an attack scenario in which attackers use a malicious file disguised as a software update or generic software. An attacker can also power a baiting attack in the physical world, such as disseminating infected USB tokens in the parking lot of a target organization and waiting for internal personnel to insert them into corporate PCs.

The malware installed on the USB tokens will compromise the PCs, gaining the full control needed for the attacks.

A quid pro quo attack (aka “something for something” attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on a specific action's execution.

In a quid pro quo attack scenario, the hacker offers a service or benefit in exchange for information or access.

The most common quid pro quo attack occurs when a hacker impersonates an IT staffer for a large organization. That hacker attempts to contact the target organization's employees via phone and then offers them some upgrade or software installation.

They might request victims to facilitate the operation by disabling the AV software temporarily to install the malicious application.

Incorrect answers:

Reverse Social Engineering

Reverse Social Engineering (RSE) is a form of social engineering attack. It has the same aim as a typical social engineering attack but with a completely different approach. This is a person-to-person attack in which an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem.

For example, the hacker establishes contact with the target through e-mail or other social media platforms, using multiple schemes and pretending to be a benefactor or skilled security personnel to convince them to provide access to their system/network. Though this technique may seem outdated and ridiculous, it has proved highly effective, especially when the victim's system/network shows signs of being compromised. Usually, in social engineering attacks, the attackers approach their targets. While in a reverse social engineering attack, the victim goes to the attacker unknowingly.

Tailgating

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. Even retina scanners don't help if an employee holds the door for an unknown person behind them out of misguided courtesy.

People who might tailgate include disgruntled former employees, thieves, vandals, mischief-makers, and issues with employees or the company. Any of these can disrupt business, cause damage, create unexpected costs, and lead to further safety issues.

Elicitation

Elicitation means to bring or draw out or arrive at a conclusion (truth, for instance) by logic. Alternatively, it is defined as stimulation that calls up (or draws forth) a particular class of behaviors, as in "the elicitation of his testimony was not easy."

In training materials, the National Security Agency of the United States government defines elicitation as "the subtle extraction of information during an apparently normal and innocent conversation."

These conversations can occur anywhere that the target is—a restaurant, the gym, a daycare—anywhere. Elicitation works well because it is low risk and often very hard to detect. Most of the time, the targets don't ever know where the information

Question 11:
John performs black-box testing. It tries to pass IRC traffic over port 80/TCP from a compromised web-enabled host during the test. Traffic is blocked, but outbound HTTP traffic does not meet any obstacles. What type of firewall checks outbound traffic?

Stateful
Packet Filtering
Circuit
Application

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

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients.

IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well.

You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls.

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

An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based.

Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.

Network-based application firewalls

Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.

Host-based application firewalls

A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

Question 12:
Which layer 3 protocol allows for end-to-end encryption of the connection?

- **SFTP**
- **IPsec**
- **SSL**
- **FTPS**

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

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

Incorrect answers:

SFTP https://en.wikipedia.org/wiki/File_Transfer_Protocol#FTP_over_SSH

FTP over SSH is the practice of tunneling a normal FTP session over a Secure Shell connection.[27] Because FTP uses multiple TCP connections (unusual for a TCP/IP protocol that is still in use), it is particularly difficult to tunnel over SSH. With many SSH clients, attempting to set up a tunnel for the control channel (the initial client-to-server connection on port 21) will protect only that channel; when data is transferred, the FTP software at either end sets up new TCP connections (data channels) and thus have no confidentiality or integrity protection.

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

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

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

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are widely used in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.

NOTE: All of these protocols are the application layer of the OSI model.

Question 13:
John, a cybersecurity specialist, received a copy of the event logs from all firewalls, Intrusion Detection Systems (IDS) and proxy servers on a company's network. He tried to match all the registered events in all the logs, and he found that their sequence didn't match. What can cause such a problem?

The security breach was a false positive.
A proper chain of custody was not observed while collecting the logs.
The network devices are not all synchronized.
The attacker altered events from the logs.

Explanation
Many network and system administrators don't pay enough attention to system clock accuracy and time synchronization. Computer clocks can run faster or slower over time, batteries and power sources die, or daylight-saving time changes are forgotten. Sure, there are many more pressing security issues to deal with, but not ensuring that the time on network devices is synchronized can cause problems. And these problems often only come to light after a security incident.

If you suspect a hacker is accessing your network, for example, you will want to analyze your log files to look for any suspicious activity. If your network's security devices do not have synchronized times, the timestamps' inaccuracy makes it impossible to correlate log files from different sources. Not only will you have difficulty in tracking events, but you will also find it difficult to use such evidence in court; you won't be able to illustrate a smooth progression of events as they occurred throughout your network.

Question 14:
Which of the following command-line flags set a stealth scan for Nmap?

-sT
-sU
-sS
-sM

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

TCP SYN (Stealth) Scan (-sS)

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

Incorrect answers:

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

UDP Scan (-sU)

While most popular services on the Internet run over the TCP protocol, UDP services are widely deployed. DNS, SNMP, and DHCP (registered ports 53, 161/162, and 67/68) are three of the most common. Because UDP scanning is generally slower and more difficult than TCP, some security auditors ignore these ports. This is a mistake, as exploitable UDP services are quite common and attackers certainly don't ignore the whole protocol. Fortunately, Nmap can help inventory UDP ports.

UDP scan is activated with the -sU option. It can be combined with a TCP scan type such as SYN scan (-sS) to check both protocols during the same run.

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

TCP Maimon Scan (-sM)

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

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

TCP Connect Scan (-sT)

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt. This and the FTP bounce scan (the section called “TCP FTP Bounce Scan (-b)”) are the only scan types available to unprivileged users.

Question 15:
The attacker posted a message and an image on the forum, in which he embedded a malicious link. When the victim clicks on this link, the victim's browser sends an authenticated request to a server. What type of attack did the attacker use?

Cross-site request forgery
Cross-site scripting
SQL injection
Session hijacking

Explanation
https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Incorrect answers:

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

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from 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.

Session hijacking https://en.wikipedia.org/wiki/Session_hijacking

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). After successfully stealing appropriate session cookies an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet. Modern web browsers use cookie protection mechanisms to protect the web from being attacked.

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.

Question 16:
The Web development team is holding an urgent meeting, as they have received information from testers about a new vulnerability in their Web software. They make an urgent decision to reduce the likelihood of using the vulnerability. The team beside to modify the software requirements to disallow users from entering HTML as input into their Web application. Determine the type of vulnerability that the test team found?

- **Cross-site scripting vulnerability.**
- **Cross-site Request Forgery vulnerability.**
- **SQL injection vulnerability.**
- **Website defacement vulnerability.**

Explanation
There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

Incorrect answers:

Website defacement vulnerability

Website defacements are the unauthorized modification of web pages, including the addition, removal, or alteration of existing content. These attacks are commonly carried out by hacktivists, who compromise a website or web server and replace or alter the hosted website information with their own messages.

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

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

Cross-site Request Forgery vulnerability https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

Question 17:
You conduct an investigation and finds out that the browser of one of your employees sent malicious requests that the employee knew nothing about. Identify the web page vulnerability that the attacker used when the attack to your employee?

File Inclusion Attack
Cross-Site Request Forgery (CSRF)
Command Injection Attacks
Hidden Field Manipulation Attack

Explanation
https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

In a CSRF attack, an innocent end-user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Incorrect answers:

Command Injection Attacks

Command injection is an attack in which the goal is the execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

File Inclusion Attack https://en.wikipedia.org/wiki/File_inclusion_vulnerability

A file inclusion vulnerability is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time. A file include vulnerability is distinct from a generic directory traversal attack, in that directory traversal is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads code for execution. Successful exploitation of a file inclusion vulnerability will result in remote code execution on the web server that runs the affected web application. An attacker can use remote code execution to create a web shell on the web server, which can be used for website defacement.

Hidden Field Manipulation Attack

Manipulating Hidden Fields: An adversary exploits a weakness in the server's trust of client-side processing by modifying data on the client-side, such as price information, and then submitting this data to the server, which processes the modified data. For example, eShoplifting is a data manipulation attack against an on-line merchant during a purchasing transaction. The manipulation of price, discount or quantity fields in the transaction message allows the adversary to acquire items at a lower cost than the merchant intended. The adversary performs a normal purchasing transaction but edits hidden fields within the HTML form response that store price or other information to give themselves a better deal. The merchant then uses the modified pricing information in calculating the cost of the selected items.

Question 18:
Identify the type of jailbreaking which allows user-level access and does not allow iboot-level access?

Userland Exploit
Bootrom Exploit
iBootrom Exploit
iBoot Exploit

Explanation
Jailbreaking can be defined as a process of installing a modified set of kernel patches that allows users to run third party applications not signed by OS vendor.

It provides root level access of the operating system and permits downloading of third-party applications, themes, extensions on an iOS devices.

It removes sandbox instructions, enabling malicious applications to get access to restricted mobile resources and information. Types of jailbreaking: Tethered, Semi- Tethered and Untethered.

Types Of jailbreaking exploits:

Userland Exploit: It allows user-level access but does not allow iboot-level access.

iBoot Exploit: An iBoot jailbreak allows user-level and iboot-level access.

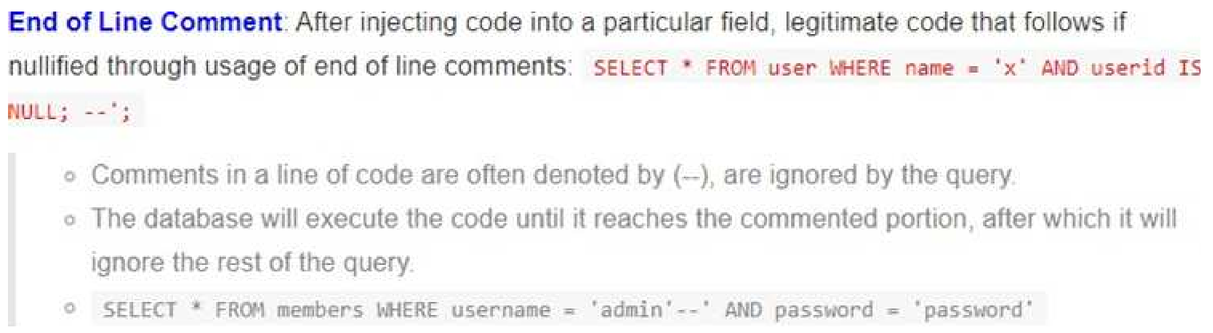
Bootrom Exploit: It allows user-level access and iboot-level access.

Question 19:
Determine the type of SQL injection:

SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --';

UNION SQL Injection.
End of Line Comment.
Tautology.
Illegal/Logically Incorrect Query.

Explanation
https://ktflash.gitbooks.io/ceh_v9/content/132_types_of_sql_injection.html

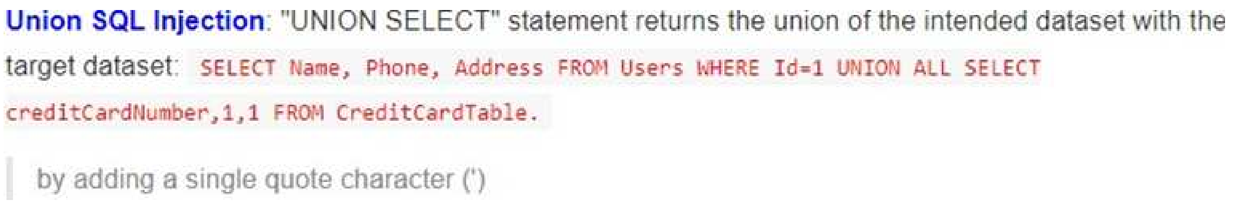


End of Line Comment: After injecting code into a particular field, legitimate code that follows if nullified through usage of end of line comments: `SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --';`

> - Comments in a line of code are often denoted by (--), are ignored by the query.
> - The database will execute the code until it reaches the commented portion, after which it will ignore the rest of the query.
> - `SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'`

Incorrect answers:

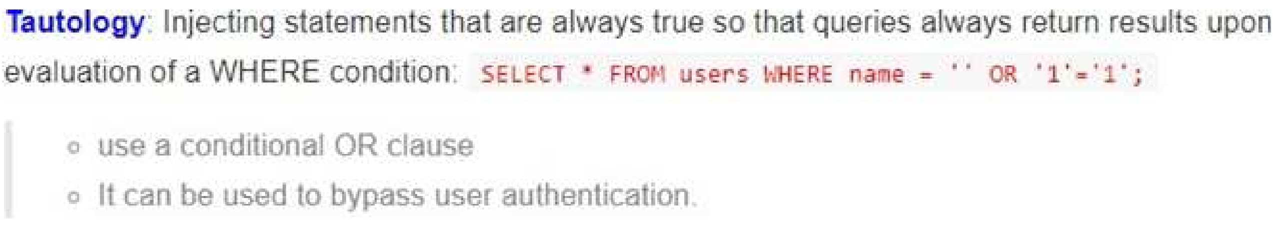
UNION SQL Injection



Union SQL Injection: "UNION SELECT" statement returns the union of the intended dataset with the target dataset: `SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable.`

> by adding a single quote character (')

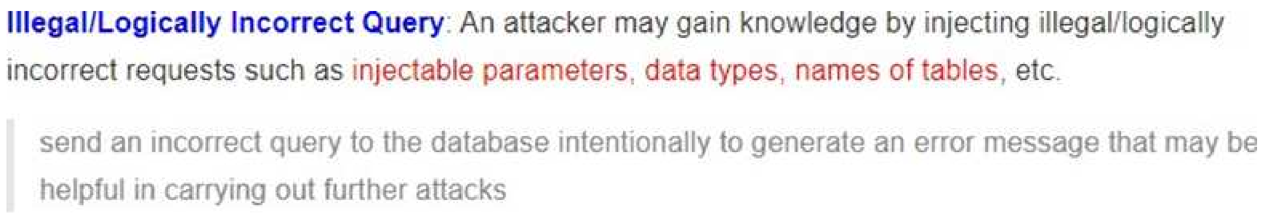
Tautology



Tautology: Injecting statements that are always true so that queries always return results upon evaluation of a WHERE condition: `SELECT * FROM users WHERE name = '' OR '1'='1';`

> - use a conditional OR clause
> - It can be used to bypass user authentication.

Illegal/Logically Incorrect Query



Illegal/Logically Incorrect Query: An attacker may gain knowledge by injecting illegal/logically incorrect requests such as injectable parameters, data types, names of tables, etc.

> send an incorrect query to the database intentionally to generate an error message that may be helpful in carrying out further attacks

Question 20:
Which of the following SQL injection attack does an attacker usually bypassing user authentication and extract data by using a conditional OR clause so that the condition of the WHERE clause will always be true?

- **UNION SQLi**
- **Error-Based SQLi**
- **End-of-Line Comment**
- **Tautology**

Explanation
In a tautology-based attack, the code is injected using the conditional OR operator such that the query always evaluates to TRUE. Tautology-based SQL injection attacks are usually bypass user authentication and extract data by inserting a tautology in the WHERE clause of a SQL query. The query transform the original condition into a tautology, causes all the rows in the database table are open to an unauthorized user. A typical SQL tautology has the form "or <comparison expression>", where the comparison expression uses one or more relational operators to compare operands and generate an always true condition. If an unauthorized user input user id as abcd and password as anything' or 'x'='x then the resulting query will be:

*select * from user_details where userid = 'abcd' and password = 'anything' or 'x'='x'*

Incorrect answers:

Error-based SQLi

The Error based technique, when an attacker tries to insert malicious query in input fields and get some error which is regarding SQL syntax or database.

For example, SQL syntax error should be like this:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ‘‘VALUE’’.

The error message gives information about the database used, where the syntax error occurred in the query. Error based technique is the easiest way to find SQL Injection.

UNION SQLi

When an application is vulnerable to SQL injection and the results of the query are returned within the application's responses, the UNION keyword can be used to retrieve data from other tables within the database. This results in an SQL injection UNION attack.

The UNION keyword lets you execute one or more additional SELECT queries and append the results to the original query. For example:

SELECT a, b FROM table1 UNION SELECT c, d FROM table2

This SQL query will return a single result set with two columns, containing values from columns a and b in table1 and columns c and d in table2.

For a UNION query to work, two key requirements must be met:

The individual queries must return the same number of columns.

The data types in each column must be compatible between the individual queries.

To carry out an SQL injection UNION attack, you need to ensure that your attack meets these two requirements.

End-of-Line Comment

After injecting code into a particular field, legitimate code that follows if nullified through the usage of end of line comments: *SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --'*;

Question 21:
Josh, a security analyst, wants to choose a tool for himself to examine links between data. One of the main requirements is to present data using graphs and link analysis. Which of the following tools will meet John's requirements?

Metasploit.
Maltego.
Analyst's Notebook.
Palantir.

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

Maltego is a software used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources and visualizing that information in a graph format, suitable for link analysis and data mining. As of 2019, the team of Maltego Technologies headquartered in Munich, Germany has taken responsibility for all global customer-facing operations.

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

Incorrect answers:

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.

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.

Analyst's Notebook https://en.wikipedia.org/wiki/Analyst%27s_Notebook

IBM Security i2 Analyst's Notebook is a software product from IBM for data analysis and investigation. Based on ELP (entity-link-property) methodology, it reveals relationships between data entities to discover patterns and provide insight into data. It is commonly used by digital analysts at law enforcement, military and other government intelligence agencies, and by fraud departments.

Palantir https://en.wikipedia.org/wiki/Palantir_Technologies

Palantir Technologies is a public American software company that specializes in big data analytics. Headquartered in Denver, Colorado, it was founded by Peter Thiel, Nathan Gettings, Joe Lonsdale, Stephen Cohen, and Alex Karp in 2003. The company's name is derived from The Lord of the Rings where the magical palantíri were "seeing-stones," described as indestructible balls of crystal used for communication and to see events in other parts of the world.

The company is known for three projects in particular: Palantir Gotham, Palantir Metropolis, and Palantir Foundry. Palantir Gotham is used by counter-terrorism analysts at offices in the United States Intelligence Community (USIC) and United States Department of Defense. In the past, Gotham was used by fraud investigators at the Recovery Accountability and Transparency Board, a former US federal agency which operated from 2009 to 2015.

Gotham was also used by cyber analysts at Information Warfare Monitor, a Canadian public-private venture which operated from 2003 to 2012. Palantir Metropolis is used by hedge funds, banks, and financial services firms. Palantir Foundry is used by corporate clients such as Morgan Stanley, Merck KGaA, Airbus, and Fiat Chrysler Automobiles NV.

Question 22:
Determine the attack according to the following scenario:

Benjamin performs a cloud attack during the translation of the SOAP message in the TLS layer. He duplicates the body of the message and sends it to the server as a legitimate user. As a result of these actions, Benjamin managed to access the server resources to unauthorized access.

Wrapping
Cloud Hopper
Cloudborne
Side-channel

Explanation
Wrapping attacks aim at injecting a faked element into the message structure so that a valid signature covers the unmodified element while the faked one is processed by the application logic. As a result, an attacker can perform an arbitrary Web Service request while authenticating as a legitimate user.

Wrapping attack which uses Extensible Mark-up Language (XML) signature element in order to weaken the web servers' validation requests. When a user requests for a service, it is interacted with using Simple Object Access Protocol (SOAP) and submitted in XML format. This type of attack usually occurs during the translation of SOAP messages in the Transport Layer Service (TLS) layer between the web server and valid user. The message body will be duplicated and sent to the server as a valid user. The hacker will copy the user's account login details. During the login session, the hackers will inject a spurious element into the message structure. They will modify the original content with malicious code. After that, the message is sent to servers. The server will approve the message as the body is unchanged. As a result, the hackers will be able to access the server resources to unauthorized access.

Incorrect answers:

Cloud Hopper

https://www.bankinfosecurity.com/report-cloud-hopper-attacks-affected-more-msps-a- 13565

The hacking campaign, known as "Cloud Hopper," was the subject of a U.S. indictment in December that accused two Chinese nationals of identity theft and fraud. Prosecutors described an elaborate operation that victimized multiple Western companies but stopped short of naming them. A Reuters report at the time identified two: Hewlett Packard Enterprise and IBM.

Cloudborne

An attack scenario affecting various cloud providers could allow an attacker to implant persistent backdoors for data theft into bare-metal cloud servers, which would be able to remain intact as the cloud infrastructure moves from customer to customer. This opens the door to a wide array of attacks on businesses that use infrastructure-as-a-service (IaaS) offerings.

Appropriately dubbed “Cloudborne” by Eclypsium, the attack vector (which the firm characterizes as a critical weakness) consists of the use of a known vulnerability in bare-metal hardware along with a weakness in the “reclamation process.”

In the Cloudborne scenario, an attacker can first use a known vulnerability in Supermicro hardware (present in many cloud providers’ infrastructure, the firm said), to overwrite the firmware of a Baseboard Management Controller (BMC). BMCs are a third-party component designed to enable remote management of a server for initial provisioning, operating system reinstall and troubleshooting.

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

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

Question 23:
Determine what of the list below is the type of honeypots that simulates the real production network of the target organization?

High-interaction Honeypots.
Pure Honeypots.
Research honeypots.
Low-interaction Honeypots.

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

Pure honeypots are full-fledged production systems. The attacker's activities are monitored by using a bug tap installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, a more controlled mechanism stealthiness of the defense mechanisms can be ensured.

Incorrect answers:

Low-interaction Honeypots

A low interaction honeypot will only give an attacker minimal access to the operating system. ‘Low interaction’ means precisely that the adversary will not be able to interact with your decoy system in any depth, as it is a much more static environment. A low interaction honeypot will usually emulate a small number of internet protocols and network services, just enough to deceive the attacker and no more. In general, most businesses simulate TCP and IP protocols, which allows the attacker to think they are connecting to a real system and not a honeypot environment.

A low interaction honeypot is simple to deploy, does not give access to a real root shell, and does not use significant resources to maintain. However, a low interaction honeypot may not be effective enough, as it is only the basic simulation of a machine. It may not fool attackers into engaging, and it’s certainly not in-depth enough to capture complex threats such as zero-day exploits.

High interaction honeypots

A high interaction honeypot emulates certain protocols or services. The attacker is provided with real systems to attack, making it far less likely they will guess they are being diverted or observed. As the systems are only present as a decoy, any traffic that is found is by its very existence malicious, making it easy to spot threats and track and trace an attacker's behavior. Using a high interaction honeypot, researchers can learn the tools an attacker uses to escalate privileges or the lateral movements they make to attempt to uncover sensitive data.

Research honeypots

Research honeypots are run to gather information about the black hat community's motives and tactics targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information and are used primarily by research, military, or government organizations.

Question 24:
Which type of viruses tries to hide from antivirus programs by actively changing and corrupting the chosen service call interruptions when they are being run?

Stealth/Tunneling virus
Cavity virus
Polymorphic virus
Tunneling virus

Explanation
Tunneling Virus: This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Stealth Virus: It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of the virus becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

NOTE: I don't know why EC-Council decided to combine 2 types of viruses into one. Nevertheless, on their exam, the Stealth/ tunneling virus (as in the book) is encountered on the exam, but I think the Tunneling virus is fine too.

Incorrect answers:

Cavity virus

To avoid detection by users, some viruses employ different kinds of deception. Some old viruses, especially on the DOS platform, make sure that the "last modified" date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date cyclic redundancy checks on file changes. Some viruses can infect files without increasing their sizes or damaging the files. They accomplish this by overwriting unused areas of executable files. These are called cavity viruses.

Polymorphic virus https://en.wikipedia.org/wiki/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.

Question 25:
Which of the following is not included in the list of recommendations of PCI Data Security Standards?

Do not use vendor-supplied defaults for system passwords and other security parameters.

Rotate employees handling credit card transactions on a yearly basis to different departments.

Protect stored cardholder data.

Encrypt transmission of cardholder data across open, public networks.

Explanation
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Build and Maintain a Secure Network

Install and maintain a firewall configuration to protect cardholder data.

Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Protect stored cardholder data.

Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Use and regularly update anti-virus software or programs.

Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Restrict access to cardholder data by business need-to-know.

Assign a unique ID to each person with computer access.

Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Track and monitor all access to network resources and cardholder data.

Regularly test security systems and processes.

Maintain an Information Security Policy

Maintain a policy that addresses information security for employees and contractors.

Question 26:
Philip, a cybersecurity specialist, needs a tool that can function as a network sniffer, record network activity, prevent and detect network intrusion. Which of the following tools is suitable for Philip?

Nmap
Cain & Abel
Snort (Correct)
Nessus

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

Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013.

Snort's open-source network-based intrusion detection/prevention system (IDS/IPS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: 1. sniffer, 2. packet logger, and 3. network intrusion detection.

Sniffer Mode

The program will read network packets and display them on the console.

Packet Logger Mode

In packet logger mode, the program will log packets to the disk.

Network Intrusion Detection System Mode

In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Incorrect answers:

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

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). 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.

Cain & Abel https://en.wikipedia.org/wiki/Cain_and_Abel

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. Cryptanalysis attacks are done via rainbow tables which can be generated with the winrtgen.exe program provided with Cain and Abel. Cain and Abel is maintained by Massimiliano Montoro and Sean Babcock.

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

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

Question 27:
Suppose your company has implemented identify people based on walking patterns and made it part of physical control access to the office. The system works according to the following principle:

The camera captures people walking and identifies employees, and then they must attach their RFID badges to access the office.

Which of the following best describes this technology?

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

Explanation
https://en.wikipedia.org/wiki/Multi-factor_authentication

The authentication factors of a multi-factor authentication scheme may include:

Something you have: Some physical object in the possession of the user, such as a security token (USB stick), a bank card, a key, etc.

Something you know: Certain knowledge only known to the user, such as a password, PIN, TAN, etc.

Something you are: Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.

Somewhere you are: Some connection to a specific computing network or using a GPS signal to identify the location.

Question 28:
Which of the following protocols is used in a VPN for setting up a secure channel between two devices?

- **PPP**
- **SET**
- **PEM**
- **IPSEC**

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

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

Incorrect answers:

PPP https://en.wikipedia.org/wiki/Point-to-Point_Protocol

Point-to-Point Protocol (PPP) is a Data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between. It can provide connection authentication, transmission encryption, and compression.

PEM https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail

Privacy-Enhanced Mail (PEM) is a file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail." While the original standards were never broadly adopted, and were supplanted by PGP and S/MIME, the textual encoding they defined became very popular. The PEM format was eventually formalized by the IETF in RFC 7468.

SET https://en.wikipedia.org/wiki/Secure_Electronic_Transaction

Secure Electronic Transaction (SET) is a communications protocol standard for securing credit card transactions over networks, specifically, the Internet. SET was not itself a payment system, but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it failed to gain attraction in the market. Visa now promotes the 3-D Secure scheme.

Question 29:
You know that the application you are attacking is vulnerable to an SQL injection, but you cannot see the result of the injection. You send a SQL query to the database, which makes the database wait before it can react. You can see from the time the database takes to respond, whether a query is true or false. What type of SQL injection did you use?
Blind SQLi.
Out-of-band SQLi.
Error-based SQLi.
UNION SQLi.

Explanation
Blind SQLi

The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

Boolean—that attacker sends a SQL query to the database prompting the application to return a result. The result will vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.

Time-based—attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The attacker can thus work out if the message they used returned true or false, without relying on data from the database.The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Incorrect answers:

Error-based SQLi

The Error based technique, when an attacker tries to insert malicious query in input fields and get some error which is regarding SQL syntax or database.

For example, SQL syntax error should be like this:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ‘‘VALUE’’.

The error message gives information about the database used, where the syntax error occurred in the query. Error based technique is the easiest way to find SQL Injection.

UNION SQLi

When an application is vulnerable to SQL injection and the results of the query are returned within the application's responses, the UNION keyword can be used to retrieve data from other tables within the database. This results in an SQL injection UNION attack.

The UNION keyword lets you execute one or more additional SELECT queries and append the results to the original query. For example:

SELECT a, b FROM table1 UNION SELECT c, d FROM table2

This SQL query will return a single result set with two columns, containing values from columns a and b in table1 and columns c and d in table2.

For a UNION query to work, two key requirements must be met:

The individual queries must return the same number of columns.

The data types in each column must be compatible between the individual queries.

To carry out an SQL injection UNION attack, you need to ensure that your attack meets these two requirements.

Out-of-band SQLi

The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

Question 30:
Which of the following tools is a command-line vulnerability scanner that scans web servers for dangerous files/CGIs?

John the Ripper
Kon-Boot
Snort
Nikto (Correct)

Explanation
https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server types 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:

Snort https://www.snort.org/

Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013.

John the Ripper https://www.openwall.com/john/

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems.

Kon-Boot https://en.wikipedia.org/wiki/Kon-Boot

Kon-Boot is a software utility that allows users to bypass Microsoft Windows passwords and Apple macOS passwords (Linux support has been deprecated) without lasting or persistent changes to system on which it is executed. It is also the first reported tool capable of bypassing Windows 10 online (live) passwords and supporting both Windows and macOS systems.

Question 31:
Which of the following application security testing method of white-box testing, in which only the source code of applications and their components is scanned for determines potential vulnerabilities in their software and architecture?

IAST
DAST
SAST
MAST

Explanation
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.

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.

Incorrect answers:

DAST https://en.wikipedia.org/wiki/Dynamic_application_security_testing

A dynamic application security testing (DAST) tool is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses. It performs a black-box test. Unlike static application security testing tools, DAST tools do not have access to the source code and therefore detect vulnerabilities by actually performing attacks.

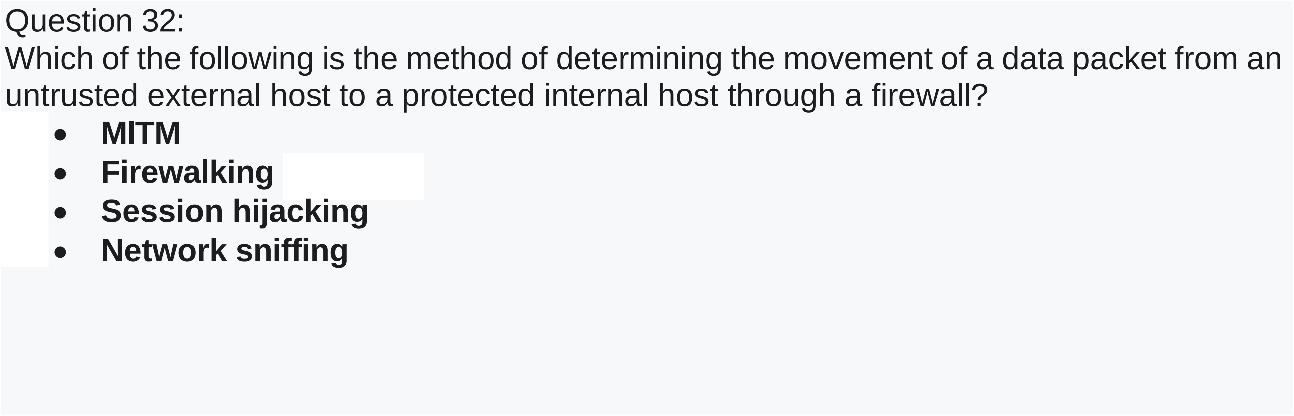
DAST tools allow sophisticated scans, detecting vulnerabilities with minimal user interactions once configured with host name, crawling parameters and authentication credentials. These tools will attempt to detect vulnerabilities in query strings, headers, fragments, verbs (GET/POST/PUT) and DOM injection.

MAST

Mobile Application Security Testing (MAST) is a blend of SAST, DAST, and forensic techniques while it allows mobile application code to be tested specifically for mobiles-specific issues such as jailbreaking, and device rooting, spoofed Wi-Fi connections, validation of certificates, data leakage prevention, etc.

IAST

Interactive Application Security Testing (IAST). Hybrid approaches have been around – combining SAST and DAST – but the cybersecurity industry has recently started to consider them under the term IAST. IAST tools can check whether known vulnerabilities (from SAST) can be exploited in a running application (i.e., DAST). These tools combine knowledge of data flow and application flow in an application to visualize advanced attack scenarios using test cases which are further used to create additional test cases by utilizing DAST results recursively.



Question 32:
Which of the following is the method of determining the movement of a data packet from an untrusted external host to a protected internal host through a firewall?

- **MITM**
- **Firewalking**
- **Session hijacking**
- **Network sniffing**

Explanation
https://en.wikipedia.org/wiki/Firewalk_(computing)

Firewalking is a technique developed by Mike Schiffman and David Goldsmith that utilizes traceroute techniques and TTL values to analyze IP packet responses in order to determine gateway ACL (Access Control List) filters and map networks. It is an active reconnaissance network security analysis technique that attempts to determine which layer 4 protocols a specific firewall will allow.

Firewalking is the method of determining the movement of a data packet from an untrusted external host to a protected internal host through a firewall.

The idea behind firewalking is to determine which ports are open and whether packets with control information can pass through a packet-filtering device.

Gathering information about a remote network protected by a firewall can be accomplished using firewalking. One of the uses of firewalking is to determine the hosts present inside the perimeter of the protected network. Another application is to determine the list of ports accessible via a firewall.

Incorrect answers:

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.

Network sniffing https://en.wikipedia.org/wiki/Sniffing_attack

Sniffing attack or a sniffer attack, in context of network security, corresponds to 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.

MITM https://en.wikipedia.org/wiki/Man-in-the-middle_attack

A man-in-the-middle (MITM) 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.

Question 33:
Often, for a successful attack, hackers very skillfully simulate phishing messages. To do this, they collect the maximum information about the company that they will attack: emails of real employees (including information about the hierarchy in the company), information

about the appearance of the message (formatting, logos), etc. What is the name of this stage of the hacker's work?

Exploration stage
Investigation stage
Reconnaissance stage
Enumeration stage

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.

NOTE: Reconnaissance takes place in two parts − Active Reconnaissance and Passive Reconnaissance. And again, the problem of the question is in the levels of abstraction. It can be difficult to choose one correct option if it is part of something larger. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) to discover and collect information about a target system covertly. "Footprinting" would have been more correct.

Question 34:
Imagine the following scenario:

1. An attacker created a website with tempting content and benner like: 'Do you want to make $10 000 in a month?'.

2. Victim clicks to the interesting and attractive content URL.

3. Attacker creates a transparent 'iframe' in front of the banner which victim attempts to click. Victim thinks that he/she clicks to the 'Do you want to make $10 000 in a month?' banner but actually he/she clicks to the content or UPL that exists in the transparent 'iframe' which is set up by the attacker.

What is the name of the attack which is described in the scenario?

- **Session Fixation**
- **Clickjacking Attack**
- **HTML Injection**
- **HTTP Parameter Pollution**

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

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

Incorrect answers:

Session Fixation https://en.wikipedia.org/wiki/Session_fixation

Session fixation is a web application attack in which attackers can trick a victim into authenticating the application using the attacker's Session Identifier. Unlike Session Hijacking, this does not rely on stealing the Session ID of an already authenticated user.

A simple way attacker can send a link containing a fixed session-id, and if the victim clicks on the link, the victim’s session id will be fixed since the attacker already know the session id so he/she can easily hijack the session.

HTML Injection https://en.wikipedia.org/wiki/Code_injection

The essence of this type of injection attack is injecting HTML code through the website's vulnerable parts. The Malicious user sends HTML code through any vulnerable field to change the website’s design or any information displayed to the user.

As a result, the user may see the data the malicious user sent. Therefore, in general, HTML Injection is just the injection of markup language code to the page's document.

Data that is being sent during this type of injection attack may be very different. It can be a few HTML tags that will display the sent information. Also, it can be the whole fake form or page. When this attack occurs, the browser usually interprets malicious user data as legit and displays it.

Changing a website’s appearance is not the only risk that this type of attack brings. It is quite similar to the XSS attack, where the malicious user steals other person’s identities. Therefore stealing another person’s identity may also happen during this injection attack.

HTTP Parameter Pollution https://en.wikipedia.org/wiki/HTTP_parameter_pollution

HTTP Parameter Pollution (HPP) is a vulnerability that occurs due to the passing of multiple parameters having the same name. There is no RFC standard on what should be done when passed multiple parameters. For example, if the parameter username is included in the GET or POST parameters twice.

Supplying multiple HTTP parameters with the same name may cause an application to interpret values in unanticipated ways. By exploiting these effects, an attacker may bypass input validation, trigger application errors, or modify internal variables values. As HTTP Parameter Pollution affects a building block of all web technologies, server and client-side attacks exist.

In 2009, immediately after the publication of the first research on HTTP Parameter Pollution, the technique received attention from the security community as a possible way to bypass web application firewalls.

Question 35:
Black hat hacker Ivan wants to implement a man-in-the-middle attack on the corporate network. For this, he connects his router to the network and redirects traffic to intercept packets. What can the administrator do to mitigate the attack?

Use the Open Shortest Path First (OSPF).
Add message authentication to the routing protocol.
Use only static routes in the corporation's network.
Redirection of the traffic is not possible without the explicit admin's confirmation.

Explanation
The area most open to attack is often the routing systems within your enterprise network. Because of some of the sniffing-based attacks, an enterprise routing infrastructure can easily be attacked with man-in-the-middle and other attacks designed to corrupt or change the routing tables with the following results:

Traffic redirection— enabling the attacker to modify traffic in transit or sniff packets;

Traffic sent to a routing black hole— the attacker can send specific routes to null0, effectively kicking IP addresses off the network;

Router denial-of-service (DoS)—attacking the routing process can crash the router or severe service degradation;

Routing protocol DoS—Similar to the attack previously described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly;

Unauthorized route prefix origination—this attack aims to introduce a new prefix into the routing table that shouldn't be there. The attacker might do this to get a covert attack network to be routable throughout the victim network.

There are four primary attack methods for these attacks:

Configuration modification of existing routers;

Introduction of a rogue router that participates in routing with legitimate routers;

Spoofing a valid routing protocol message or modifying a valid message in transit;

Sending of malformed or excess packets to a routing protocol process.

These four attack methods can be mitigated in the following ways:

To counter configuration modification of existing routers, you must secure the routers. This includes not only the configuration of the router but also the supporting systems it makes use of, such as TFTP servers.

Anyone can attempt to introduce a rogue router, but to cause damage, the attacker needs the other routing devices to believe the sent information. This can most easily be blocked by adding message authentication to your routing protocol. Additionally, the routing protocol message types can be blocked by ACLs from networks with no need to originate them.

Message authentication can also help prevent the spoofing or modification of a valid routing protocol message. Besides, the transport layer protocol (such as TCP for BGP) can further complicate message spoofing because of the difficulty in guessing pseudo-random initial sequence numbers (assuming a remote attacker).

Excess packets can be stopped through the use of traditional DoS mitigation techniques. Malformed packets, however, are nearly impossible to stop without the participation of the router vendor. Only through exhaustive testing and years of field use do routing protocol implementations correctly deal with most malformed messages. This is an area of computer security that needs increased attention, not just in routing protocols but in all network applications.

Question 36:
Which of the options presented below is not a Bluetooth attack?

Bluesmacking
Bluesnarfing
Bluejacking
Bluedriving

Explanation
https://github.com/verovaleros/bluedriving

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

Incorrect answers:

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

Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs, or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or blue chat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but it's possible to send images or sounds with modern phones. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking is also confused with Bluesnarfing, which is how mobile phones are illegally hacked via Bluetooth.

NOTE: There are several problems with this option:

This is not feasible on modern smartphones. It was a long time ago. Why know this in 2019-2021 is not clear, even as a simple history.

This is not an attack at all.

Bluesmacking

One of the older types of attacks against Bluetooth. This attack is a variation of a common attack against networks, devices, and applications known as a Denial-of-service.

The specially crafted packet can make a device unusable. This attack works by transmitting a data packet that exceeds the maximum packet size available on Bluetooth devices. The result is that the device cannot process the packet, and the target becomes the victim of a Denial-of-service.

NOTE: Old... but not Obsolete.

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

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

Question 37:
You analyze the logs and see the following output of logs from the machine with the IP address of 192.168.0.132:

```
Time August 21 11:22:06 Port:20 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:08 Port:21 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:11 Port:22 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:14 Port:23 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:15 Port:25 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:19 Port:80 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
Time August 21 11:22:21 Port:443 Source:192.168.0.30 Destination:192.168.0.132 Protocol:TCP
```

What conclusion can you make based on this output?

Denial of service attack targeting 192.168.0.132
Port scan targeting 192.168.0.30
Teardrop attack targeting 192.168.0.132
Port scan targeting 192.168.0.132

Explanation
https://nmap.org/book/nmap-defenses-detection.html

As we can see in the image from IP 192.168.0.30 a lot of requests are received to IP 192.168.0.132 on different ports 20, 21, 22, etc.

Based on this, we can conclude that a port scan is being performed at 192.168.0.132**.**

Question 38:
With which of the following SQL injection attacks can an attacker deface a web page, modify or add data stored in a database and compromised data integrity?

- **Unauthorized access to an application.**
- **Compromised Data Integrity.**
- **Loss of data availability.**
- **Information Disclosure.**

Explanation
With a successful attack using SQL injection, an attacker can gain:

Compromised data integrity. As SQL statements are also used to modify or add the record, an attacker can use SQL injection to modify or add data stored in a database. This would lead to compromised data integrity.

Unauthorized access to an application. An attacker can successfully bypass an application's authentication mechanism to have illegitimate access to it.

Information disclosure. An attack could lead to a complete data leakage from the database server.

Loss of data availability. An attacker can delete records from the database server.

Question 39:
The attacker enters its malicious data into intercepted messages in a TCP session since source routing is disabled. He tries to guess the responses of the client and server. What hijacking technique is described in this example?

RST
TCP/IP
Blind
Registration

Explanation
https://www.greycampus.com/opencampus/ethical-hacking/network-or-tcp-session-hijacking?sscid=c1k4_w62kp

In cases where source routing is disabled, the session hijacker can also use blind hijacking where he injects his malicious data into intercepted communications in the TCP session. It is called blind because he cannot see the response; though the hijacker can send the data or commands, he is basically guessing the responses of the client and server.

Incorrect answers:

TCP/IP

TCP Hijacking - A type of Man-in-the-Middle attack where an attacker is able to view the packets of the network participants and send their own packets to the network. The attack takes advantage of the TCP connection establishment features and can be carried out both during the "triple handshake" and when the connection is established.

The problem of possible spoofing of a TCP message is important since an analysis of the FTP and TELNET protocols implemented on the basis of the TCP protocol showed that the problem of identifying FTP and TELNET packets is entirely assigned by these protocols to the transport layer, that is, to TCP.

RST

RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgement number. The hacker can reset the victim's connection if it uses an accurate acknowledgement number.

Registration

Registration hijacking refers to the action of an attacker to register himself as the targeted VoIP user. If successful, all the incoming calls to the victim VoIP user will be routed to the VoIP phone chosen by the attacker rather than the victim's VoIP phone. In other words, the attacker rather than the victim will receive all the incoming calls to the victim. In this section, we describe how attacker could hijack the VoIP registration and discuss why currently deployed systems are vulnerable.

Question 40:
The attacker tries to take advantage of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Which of the following queries best describes an attempt to exploit an insecure direct object using the name of the valid account "User 1"?

"GET/restricted/bank.getaccount("˜User1') HTTP/1.1 Host: westbank.com"

"GET/restricted/goldtransfer?to=Account&from=1 or 1=1' HTTP/1.1Host: westbank.com"

"GET/restricted/\r\n\%00account%00User1%00access HTTP/1.1 Host: westbank.com"

"GET/restricted/accounts/?name=User1 HTTP/1.1 Host: westbank.com"

Explanation
This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account. Below you will find more detailed information about IDOR vulnerability.

Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.

Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.

The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it’s necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let’s say that the web application displays transaction details using the following URL:

```
https://www.example.com/transaction.php?id=74656
```

A malicious hacker could try to substitute the *id* parameter value 74656 with other similar
values, for example:

```
https://www.example.com/transaction.php?id=74657
```

The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

Question 41:
What actions should be performed before using a Vulnerability Scanner for scanning a network?

TCP/IP stack fingerprinting.
Checking if the remote host is alive.
TCP/UDP Port scanning.
Firewall detection.

Explanation
Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.

Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.

Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

Question 42:
Which of the following is the risk that remains after the amount of risk left over after natural or inherent risks have been reduced?

- **Residual risk**
- **Impact risk**
- **Inherent risk**
- **Deferred risk**

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

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

· **Residual risk = (Inherent risk) – (impact of risk controls)**

Question 43:
Which of the following incident handling process phases is responsible for defining rules, employees training, creating a back-up, and preparing software and hardware resources before an incident occurs?

Recovery
Containment
Identification
Preparation

Explanation
Preparation

Among the most important of all the steps in an incident response plan is the preparation stage. During the preparation phase, organizations should establish policies and procedures for incident response management and enable efficient communication methods both before and after the incident.

Employees should be properly trained to address security incidents and their respective roles. Companies need to develop incident response drill scenarios that are practiced regularly and modified as needed based on changes in the environment. All aspects of an incident response plan, including training, software and hardware resources, and execution, should be fully approved and funded before an incident occurs.

Identification

The identification phase of an incident response plan involves determining whether or not an organization has been breached. It is not always clear at first whether a breach or other security incident has occurred. Besides, breaches can originate from a wide range of sources, so it is important to gather details. When determining whether a security incident has occurred, organizations should look at when the event happened, how it was discovered, and who discovered the breach. Companies should also consider how the incident will impact operations if other areas have been impacted and the compromise's scope.

Containment

If it is discovered that a breach has occurred, organizations should work fast to contain the event. However, this should be done appropriately and does not require all sensitive data to be deleted from the system. Instead, strategies should be developed to contain the breach and prevent it from spreading further. This may involve disconnecting the impacted device from the internet or having a back-up system that can be used to restore normal business operations. Having remote access protocols in place can help ensure that a company never loses access to its system.

Neutralization

Neutralization is one of the most crucial phases of the incident response process and requires the intelligence gathered throughout the previous stages. Once all systems and devices that have been impacted by the breach have been identified, an organization should perform a coordinated shutdown.

To ensure that all employees are aware of the shutdown, employers should send out notifications to all other IT team members. Next, the infected systems and devices should be wiped clean and rebuilt. Passwords on all accounts should also be changed. If a business discovers that there are domains or IP addresses that have been affected, it is essential to block all communication that could pose a risk.

Recovery

The recovery phase of an incident response plan involves restoring all affected systems and devices to allow for normal operations to continue. However, before getting systems back up and running, it is vital to ensure that the breach's cause has been identified to prevent another breach from occurring again. During this phase, consider how long it will take to return systems to normal, whether systems have been patched and tested, whether a system can be safely restored using a backup, and how long the system will need to be monitored.

Review

The final step in an incident response plan occurs after the incident has been solved. Throughout the incident, all details should have been properly documented so that the information can be used to prevent similar breaches in the future. Businesses should complete a detailed incident report that suggests tips on how to improve the existing incident plan. Companies should also closely monitor any post-incident activities to look for threats. It is important to coordinate across all departments of an organization so that all employees are involved and can do their part to help prevent future security incidents.

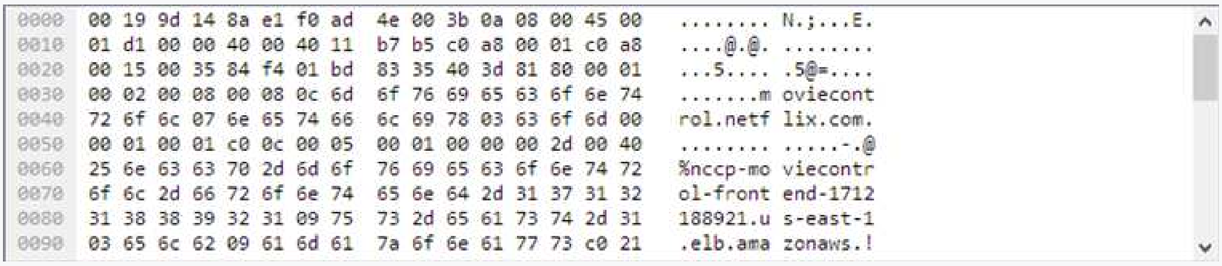
Question 44:
Wireshark is one of the most important tools for a cybersecurity specialist. It is used for network troubleshooting, analysis, software, etc. And you often have to work with a packet bytes pane. In what format is the data presented in this pane?

- **ASCII only**
- **Hexadecimal**
- **Binary**
- **Decimal**

Explanation
https://www.wireshark.org/docs/wsug_html_chunked/ChUsePacketBytesPaneSection.html

The packet bytes pane shows the data of the current packet in a hexdump style.

hexdump is a hexadecimal view (on screen or paper) of computer data, from RAM or from a computer file or storage device.



```
0000  00 19 9d 14 8a e1 f0 ad  4e 00 3b 0a 08 00 45 00   ........ N.;...E.
0010  01 d1 00 00 40 00 40 11  b7 b5 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 15 00 35 84 f4 01 bd  83 35 40 3d 81 80 00 01   ...5.... .5@=....
0030  00 02 00 08 00 08 0c 6d  6f 76 69 65 63 6f 6e 74   .......m oviecont
0040  72 6f 6c 07 6e 65 74 66  6c 69 78 03 63 6f 6d 00   rol.netf lix.com.
0050  00 01 00 01 c0 0c 00 05  00 01 00 00 00 2d 00 40   ........ .....-.@
0060  25 6e 63 63 70 2d 6d 6f  76 69 65 63 6f 6e 74 72   %nccp-mo viecontr
0070  6f 6c 2d 66 72 6f 6e 74  65 6e 64 2d 31 37 31 32   ol-front end-1712
0080  31 38 38 39 32 31 09 75  73 2d 65 61 73 74 2d 31   188921.u s-east-1
0090  03 65 6c 62 09 61 6d 61  7a 6f 6e 61 77 73 c0 21   .elb.ama zonaws.!
```

Question 45:
Alex, a cyber security specialist, should conduct a pentest inside the network, while he received absolutely no information about the attacked network. What type of testing will Alex conduct?

Internal, Black-box.
External, Black-box.
Internal, Grey-box.
Internal, White-box.

Explanation
https://en.wikipedia.org/wiki/Black-box_testing

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied virtually to every level of software testing: unit, integration, system, and acceptance. It is sometimes referred to as specification-based testing.

Specific knowledge of the application's code, internal structure, and programming knowledge, in general, is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

Question 46:
Victor, a white hacker, received an order to perform a penetration test from the company "Test us".

He starts collecting information and finds the email of an employee of this company in free access. Victor decides to send a letter to this email, changing the original email address to the email of the boss of this employee, "boss@testus.com". He asks the employee to immediately open the "link with the report" and check it. An employee of the company "Test us" opens this link and infects his computer.

Thanks to these manipulations, Viktor gained access to the corporate network and successfully conducted a pentest.

What type of attack did Victor use?

Eavesdropping
Piggybacking
Social engineering
Tailgating

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:

Tailgating and Piggybacking are the same thing

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. Even retina scanners don't help if an employee holds the door for an unknown person behind them out of misguided courtesy.

People who might tailgate include disgruntled former employees, thieves, vandals, mischief-makers, and issues with employees or the company. Any of these can disrupt business, cause damage, create unexpected costs, and lead to further safety issues.

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

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information. Since the beginning of the digital age, the term has also come to hold great significance in the world of cybersecurity.

The question does not specify at what level and how this attack is used. An attacker can eavesdrop on a conversation or use special software and obtain information on the network. There are many options, but this is not important because the correct answer is clearly not related to information interception.

Question 47:
Which of the following Nmap's commands allows you to most reduce the probability of detection by IDS when scanning common ports?

nmap -sT -O -T0
nmap -A --host-timeout 99-T1
nmap -sT -O -T2
nmap -A – Pn

Explanation
https://nmap.org/book/man-performance.html

Nmap offers a simple approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). The first two are for IDS evasion. Polite mode slows down the scan to use less bandwidth and target machine resources. Normal mode is the default and so -T3 does nothing. Aggressive mode speeds scans up by making the assumption that you are on a reasonably fast and reliable network. Finally insane mode assumes that you are on an extraordinarily fast network or are willing to sacrifice some accuracy for speed.

NOTE: The trick here is to choose the slowest scan. And here everything is obvious (T0). Without an explicit indication of the speed, the default mode (T3).

Question 48:
Which of the following is a network software suite designed for 802.11 WEP and WPA-PSK keys cracking that can recover keys once enough data packets have been captured?

- **Aircrack-ng**
- **WLAN-crack**
- **Airguard**
- **Wificracker**

Explanation
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.

Question 49:
Which of the following best describes code injection?

Form of attack in which a malicious user gains access to the codebase on the server and inserts new code.

Form of attack in which a malicious user inserts additional code into the JavaScript running in the browser.

Form of attack in which a malicious user gets the server to execute arbitrary code using a buffer overflow.

Form of attack in which a malicious user inserts text into a data field interpreted as code.

Explanation

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection can be disastrous, for example by allowing computer worms to propagate.

Code injection vulnerabilities occur when an application sends untrusted data to an interpreter. Injection flaws are most often found in SQL, LDAP, XPath, or NoSQL queries; OS commands; XML parsers, SMTP headers, program arguments, etc. Injection flaws tend to be easier to discover when examining source code than via testing. Scanners and fuzzers can help find injection flaws.

Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.

Question 50:
John, a pentester, received an order to conduct an internal audit in the company. One of its tasks is to search for open ports on servers. Which of the following methods is the best solution for this task?

- **Scan servers with Nmap.**
- **Scan servers with MBSA.**
- **Manual scan on each server.**
- **Telnet to every port on each server.**

Explanation

https://nmap.org/book/port-scanning-tutorial.html

The correct answer is “Scan servers with Nmap” because Nmap combines high speed of work and keeps the most common usage simple while retaining the flexibility for custom and advanced scans which accomplished with the command-line interface by offering dozens of options, but choosing sane defaults when they are not specified.

Question 51:
Alex, the penetration tester, performs a server scan. To do this, he uses the method where the TCP Header is split into many packets so that it becomes difficult to determine what packages are used for. Determine the scanning technique that Alex uses?

ACK flag scanning

TCP Scanning

IP Fragmentation Scan (

Inverse TCP flag scanning

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

IP fragmentation attacks are a kind of computer security attack based on how the Internet Protocol (IP) requires data to be transmitted and processed. Specifically, it invokes IP fragmentation, a process used to partition messages (the service data unit (SDU); typically a packet) from one layer of a network into multiple smaller payloads that can fit within the lower layer's protocol data unit (PDU). Every network link has a maximum size of messages that may be transmitted, called the maximum transmission unit (MTU). If the SDU plus metadata added at the link-layer exceeds the MTU, the SDU must be fragmented. IP fragmentation attacks exploit this process as an attack vector.

Part of the TCP/IP suite is the Internet Protocol (IP) which resides at the Internet Layer of this model. IP is responsible for the transmission of packets between network end points. IP includes some features which provide basic measures of fault-tolerance (time to live, checksum), traffic prioritization (type of service) and support for the fragmentation of larger packets into multiple smaller packets (ID field, fragment offset). The support for fragmentation of larger packets provides a protocol allowing routers to fragment a packet into smaller packets when the original packet is too large for the supporting datalink frames. IP fragmentation exploits (attacks) use the fragmentation protocol within IP as an attack vector.

Incorrect answers:

ACK scanning https://en.wikipedia.org/wiki/Port_scanner#ACK_scanning

ACK scanning is one of the more unusual scan types, as it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This is especially good when attempting to probe for the existence of a firewall and its rulesets. Simple packet filtering will allow established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not.

TCP scanning https://en.wikipedia.org/wiki/Port_scanner#TCP_scanning

The simplest port scanners use the operating system's network functions and are generally the next option to go to when SYN is not a feasible option (described next). Nmap calls this mode connect scan, named after the Unix connect() system call. If a port is open, the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection to avoid performing a Denial-of-service attack. Otherwise an error code is returned. This scan mode has the advantage that the user does not require special privileges. However, using the OS network functions prevents low-level control, so this scan type is less common. This method is "noisy", particularly if it is a "portsweep": the services can log the sender IP address and Intrusion detection systems can raise an alarm.

Inverse TCP flag scanning

Inverse TCP flag scanning works by sending TCP probe packets with or without TCP flags. Based on the response, it is possible to determine whether the port is open or closed. If there is no response, then the port is open. If the response is RST, then the port is closed.

Question 52:
Which of the following is an encryption technique where data is encrypted by a sequence of photons that have a spinning trait while travelling from one end to another?

- **Hardware-Based.**
- **Quantum Cryptography.**

Homomorphic.
Elliptic Curve Cryptography.

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

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is a quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution.

Quantum key distribution

The best-known and developed application of quantum cryptography is a quantum key distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, discrepancies will arise causing Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography.

The security of quantum key distribution can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with the classical key distribution. This is usually described as "unconditional security", although there are some minimal assumptions required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise, a man-in-the-middle attack would be possible.

While QKD is seemingly secure, its applications face the challenge of practicality. This is due to transmission distance and key generation rate limitations. Ongoing studies and growing technology has allowed further advancements in such limitations. In 2018 Lucamarini et al. proposed a twin-field QKD scheme that can possibly overcome the point-to-point repeater-less bounds of a lossy communication channel. The rate of the twin field protocol was shown to overcome the repeater-less PLOB bound at 340 km of an optical fibre; its ideal rate surpasses this bound already at 200 km and follows the rate-loss scaling of the higher single-repeater bound. The protocol suggests that optimal key rates are achievable on "550 kilometres of standard optical fibre", which is already commonly used in communications today. The theoretical result was confirmed in the first experimental demonstration of QKD beyond the rate-loss limit by Minder et al. in 2019, which has been characterised as the first effective quantum repeater.

Quantum coin flipping

Unlike quantum key distribution, quantum coin flipping is a protocol that is used between two participants who do not trust each other. The participants communicate via a quantum channel and exchange information through the transmission of qubits. But because Alice and Bob do not trust each other, each expects the other to cheat. Therefore, more effort must be spent on ensuring that neither Alice nor Bob can gain a significant advantage over the other to produce the desired outcome. An ability to influence a particular outcome is referred to as a bias, and there is a significant focus on developing protocols to reduce the bias of a dishonest player, otherwise known as cheating. Quantum communication protocols, including quantum coin flipping, have been shown to provide significant security advantages over classical communication, though they are difficult to realize in the practical world.

A coin flip protocol generally occurs like this:

Alice chooses a basis (either rectilinear or diagonal) and generates a string of photons to send to Bob in that basis.

Bob randomly chooses to measure each photon in a rectilinear or diagonal basis, noting which basis he used and the measured value.

Bob publicly guesses which basis Alice used to send her qubits.

Alice announces the basis she used and sends her original string to Bob.

Bob confirms by comparing Alice's string to his table. It should be perfectly correlated with the values Bob measured using Alice's basis and completely uncorrelated with the opposite.

Cheating occurs when one player attempts to influence, or increase the probability of a particular outcome. The protocol discourages some forms of cheating; for example, Alice could cheat at step 4 by claiming that Bob incorrectly guessed her initial basis when he guessed correctly, but Alice would then need to generate a new string of qubits that perfectly correlates with what Bob measured in the opposite table.Her chance of generating a matching string of qubits will decrease exponentially with the number of qubits sent, and if Bob notes a mismatch, he will know she was lying. Alice could also generate a string of photons using a mixture of states, but Bob would easily see that her string will correlate partially (but not fully) with both sides of the table, and know she cheated in the process. There is also an inherent flaw that comes with current quantum devices. Errors and lost qubits will affect Bob's measurements, resulting in holes in Bob's measurement table. Significant losses in measurement will affect Bob's ability to verify Alice's qubit sequence in step 5.

One theoretically surefire way for Alice to cheat is to utilize the Einstein-Podolsky-Rosen (EPR) paradox. Two photons in an EPR pair are anticorrelated; that is, they will always be found to have opposite polarizations, provided that they are measured on the same basis. Alice could generate a string of EPR pairs, sending one photon per pair to Bob and storing the other herself. When Bob states his guess, she could measure her EPR pair photons in the opposite basis and obtain a perfect correlation to Bob's opposite table. Bob would never know she cheated. However, this requires capabilities that quantum technology currently does not possess, making it impossible to do in practice. To successfully execute this, Alice would need to be able to store all the photons for a significant amount of time as well as to measure them with near-perfect efficiency. This is because any photon lost in storage or in measurement would result in a hole in her string that she would have to fill by guessing. The more guesses she has to make, the more she risks detection by Bob for cheating.

Question 53:
Identify the standard by the description:

A regulation contains a set of guidelines that everyone who processes any electronic data in medicine should adhere to. It includes information on medical practices, ensuring that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to secure patient data.

COBIT
ISO/IEC 27002
HIPAA
FISMA

Explanation
Correct answer: HIPAA

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

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

The act consists of five titles.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Title III sets guidelines for pre-tax medical spending accounts.

Title IV sets guidelines for group health plans, and Title V governs company-owned life insurance policies.

Incorrect answers:

FISMA https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

The Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347 (text) (pdf), 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. In FY 2008, federal agencies spent $6.2 billion securing the government's total information technology investment of approximately $68 billion or about 9.2 percent of the total information technology portfolio.

ISO/IEC 27002 https://en.wikipedia.org/wiki/ISO/IEC_27002

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), titled Information technology – Security techniques – Code of practice for information security controls.

The ISO/IEC 27000-series standards are descended from a corporate security standard donated by Shell to a UK government initiative in the early 1990s.[1] The Shell standard was developed into British Standard BS 7799 in the mid-1990s, and was adopted as ISO/IEC 17799 in 2000. The ISO/IEC standard was revised in 2005, and renumbered ISO/IEC 27002 in 2007 to align with the other ISO/IEC 27000-series standards. It was revised again in 2013. Later in 2015 the ISO/IEC 27017 was created from that standard in order to suggesting additional security controls for the cloud which were not completely defined in ISO/IEC 27002.

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

COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for information technology (IT) management and IT governance.

The framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.

Question 54:
You makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions. What type of attack are you trying to perform?

Chosen-plaintext attack
Ciphertext-only attack
Known-plaintext attack
Adaptive chosen-plaintext attack

Explanation
A shape adaptive chosen-plaintext attack is a chosen-plaintext attack scenario in which the attacker has the ability to make his choice of the inputs to the encryption function based on the previous chosen-plaintext queries and their corresponding ciphertexts. The scenario is clearly more powerful than the basic chosen-plaintext attack but is probably less practical in real life since it requires the interaction of the attacker with the encryption device.

Incorrect answers:

Chosen-plaintext attack 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.

Modern ciphers aim to provide semantic security, also known as ciphertext indistinguishability under chosen-plaintext attack and are therefore by design generally immune to chosen-plaintext attacks if correctly implemented.

Ciphertext-only attack https://en.wikipedia.org/wiki/Ciphertext-only_attack

A ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. While the attacker has no channel providing access to the plaintext prior to encryption, in all practical ciphertext-only attacks, the attacker still has some knowledge of the plaintext. For instance, the attacker might know the language in which the plaintext is written or the expected statistical distribution of characters in the plaintext. Standard protocol data and messages are commonly part of the plaintext in many deployed systems and can usually be guessed or known efficiently as part of a ciphertext-only attack on these systems.

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

A 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 codebooks.

Question 55:
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

Can identify unknown attacks.
Produces less false positives.
Cannot deal with encrypted network traffic.
Requires vendor updates for a new threat.

Explanation
https://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system

An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.

Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.

Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

Question 56:
Which of the following is a protocol that used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system?

CAPTCHA
Internet Engineering Task Force
Internet Assigned Numbers Authority
WHOIS

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

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

Incorrect answers:

Internet Assigned Numbers Authority

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

The Internet Assigned Numbers Authority (IANA) is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers.

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

A CAPTCHA (a contrived acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge–response test used in computing to determine whether or not the user is human.

Internet Engineering Task Force

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

The Internet Engineering Task Force (IETF) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). It has no formal membership roster or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.

The IETF started out as an activity supported by the federal government of the United States, but since 1993 it has operated as a standards-development function under the auspices of the Internet Society, an international membership-based non-profit organization.

Question 57:
Elon plans to make it difficult for the packet filter to determine the purpose of the packet when scanning. Which of the following scanning techniques will Elon use?

ACK scanning.
IPID scanning.
ICMP scanning.
SYN/FIN scanning using IP fragments.

Explanation
SYN/FIN scanning using IP fragments is a process of scanning that was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

Incorrect answers:

ICMP scanning

The Internet Control Message Protocol (ICMP) is like the TCP protocol; both support protocols in the internet protocol suite. ICMP is used for checking live systems; ping is the most well-known utility that uses ICMP requests. Its principle is very simple—ICMP scanning sends requests to hosts and waits for an echo request to check whether the system is alive.

ACK scanning

ACK scanning is one of the more unusual scan types, as it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This is especially good when attempting to probe for the existence of a firewall and its rulesets.

IPID scanning https://en.wikipedia.org/wiki/Idle_scan

Idle scans take advantage of predictable Identification field value from IP header: every IP packet from a given source has an ID that uniquely identifies fragments of an original IP datagram; the protocol implementation assigns values to this mandatory field generally by a fixed value (1) increment. Because transmitted packets are numbered in a sequence you can say how many packets are transmitted between two packets that you receive.

An attacker would first scan for a host with a sequential and predictable sequence number (IPID). The latest versions of Linux, Solaris, OpenBSD, and Windows Vista are not suitable as zombie, since the IPID has been implemented with patches that randomized the IPID. Computers chosen to be used in this stage are known as "zombies".

Once a suitable zombie is found the next step would be to try to establish a TCP connection with a given service (port) of the target system, impersonating the zombie. It is done by sending a SYN packet to the target computer, spoofing the IP address from the zombie, i.e. with the source address equal to zombie IP address.

If the port of the target computer is open it will accept the connection for the service, responding with a SYN/ACK packet back to the zombie.

The zombie computer will then send a RST packet to the target computer (to reset the connection) because it did not actually send the SYN packet in the first place.

Since the zombie had to send the RST packet it will increment its IPID. This is how an attacker would find out if the target's port is open. The attacker will send another packet to the zombie. If the IPID is incremented only by a step then the attacker would know that the particular port is closed.

The method assumes that zombie has no other interactions: if there is any message sent for other reasons between the first interaction of the attacker with the zombie and the second interaction other than RST message, there will be a false positive.

Question 58:
Which of the following will allow you to prevent unauthorized network access to local area networks and other information assets by wireless devices?

HIDS
AISS
WIPS
NIDS
Explanation

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

A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

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, similar to the way a network-based intrusion detection system (NIDS) operates. This was the first type of intrusion detection software to have been designed, with the original target system being the mainframe computer where outside interaction was infrequent.

NIDS https://en.wikipedia.org/wiki/Intrusion_detection_system#Network_intrusion_detection_systems

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. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulating network intrusion detection systems. NIDS are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real-time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

AIDS

Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Since these models can be trained according to the applications and hardware configurations, machine learning based method has a better generalized property in comparison to traditional signature-based IDS. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious. Most of the existing IDSs suffer from the time-consuming during detection process that degrades the performance of IDSs. Efficient feature selection algorithm makes the classification process used in detection more reliable.

Question 59:
Identify Secure Hashing Algorithm, which produces a 160-bit digest from a message on principles similar to those used in MD4 and MD5?

SHA-2
SHA-1
SHA-0
SHA-3

Explanation
Correct answer: SHA-1

Explanation: https://en.wikipedia.org/wiki/SHA-1

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD2, MD4 and MD5 message digest algorithms, but generates a larger hash value (160 bits vs. 128 bits).

Incorrect answers:

SHA-0 https://en.wikipedia.org/wiki/SHA-1#SHA-0

The original algorithm specification was published in 1993 as the Secure Hash Standard (FIPS PUB 180). This version is known as SHA-0 and soon after the issue was withdrawn by NSA which made the change on it. The change concerned the rotation bits left by n positions and should contribute to greater security. April 17, 1995 it was granted a standard and the version known as SHA-1 (FIPS PUB 180-1).

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

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. They are built using the Merkle–Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4.

SHA-2 was first published by the National Institute of Standards and Technology (NIST) as a U.S. federal standard (FIPS). The SHA-2 family of algorithms are patented in US patent 6829355. The United States has released the patent under a royalty-free license.

SHA-3 https://en.wikipedia.org/wiki/SHA-3

SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. Although part of the same series of standards, SHA-3 is internally different from the MD5-like structure of SHA-1 and SHA-2.

SHA-3 is a subset of the broader cryptographic primitive family Keccak (/ˈkɛtʃæk/ or /ˈkɛtʃɑːk/), designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, building upon RadioGatún. Keccak's authors have proposed additional uses for the function, not (yet) standardized by NIST, including a stream cipher, an authenticated encryption system, a "tree" hashing scheme for faster hashing on certain architectures, and AEAD ciphers Keyak and Ketje.

Keccak is based on a novel approach called sponge construction.Sponge construction is based on a wide random function or random permutation, and allows inputting ("absorbing" in sponge terminology) any amount of data, and outputting ("squeezing") any amount of data, while acting as a pseudorandom function with regard to all previous inputs. This leads to great flexibility.

Question 60:
Ivan, the black hat hacker, split the attack traffic into many packets such that no single packet triggers the IDS. Which IDS evasion technique does Ivan use?

- **Unicode Evasion.**
- **Session Splicing.**
- **Low-bandwidth attacks.**
- **Flooding.**

Explanation
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

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

Incorrect answers:

Unicode invasion

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.

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

Flood attacks are also known as Denial of Service (DoS) attacks. In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all its resources to send reply commands.

Low-bandwidth attacks https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Low-bandwidth_attacks

Attacks which are spread out across a long period of time or a large number of source IPs, such as nmap's slow scan, can be difficult to pick out of the background of benign traffic. An online password cracker which tests one password for each user every day will look nearly identical to a normal user who mistyped their password.

Question 61:
Which of the following tools is packet sniffer, network detector and IDS for 802.11(a, b, g, n) wireless LANs?

Abel
Nessus
Nmap
Kismet

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

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

Incorrect answers:

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

Nessus is a remote security scanning tool that scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to access any computer you have connected to a network.

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

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). 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.

Abel https://en.wikipedia.org/wiki/Cain_and_Abel_(software)

Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could 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. Cryptanalysis attacks were done via rainbow tables which could be generated with the winrtgen.exe program provided with Cain and Abel.

Question 62:
What is the purpose of the demilitarized zone?

To add a protect to network devices.
To scan all traffic coming through the DMZ to the internal network.
To provide a place for a honeypot.
To add an extra layer of security to an organization's local area network.

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

DMZ Network (demilitarized zone) functions as a subnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to untrusted networks, commonly the Internet.

The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ. In contrast, the rest of the organization's network is safe behind a firewall.

When implemented properly, a DMZ Network gives organizations extra protection to detect and mitigate security breaches before they reach the internal network, where valuable assets are stored.

Question 63:
You managed to compromise a server with an IP address of 10.10.0.5, and you want to get fast a list of all the machines in this network. Which of the following Nmap command will you need?

nmap -T4 -F 10.10.0.0/24
nmap -T4 -r 10.10.1.0/24
nmap -T4 -q 10.10.0.0/24
nmap -T4 -p 10.10.0.0/24

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

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

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

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

Question 64:
Attacker uses various IDS evasion techniques to bypass intrusion detection mechanisms. At the same time, IDS is configured to detect possible violations of the security policy, including unauthorized access and misuse. Which of the following evasion method depend on the Time-to-Live (TTL) fields of a TCP/IP ?

Obfuscation
Unicode Evasion
Denial-of-Service Attack
Insertion Attack

Explanation
According to the EC-Council's study guides, the Insertion Attack looks like this: The attacker can send packets whose time-to-live (TTL) fields are crafted to reach the IDS but not the target computers. This will result in the IDS and the target system having two different character strings. An attacker confronts the IDS with a stream of one-character packets (the attacker-originated data stream), in which one of the characters (the letter “X”) will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

More information about Insertion Attack:

An IDS can accept a packet that an end-system rejects. An IDS that does this makes the mistake of believing that the end-system has accepted and processed the packet when it actually hasn't. An attacker can exploit this condition by sending packets to an end-system that it will reject, but that the IDS will think are valid. In doing this, the attacker is "inserting" data into the IDS --- no other system on the network cares about the bad packets.

It calls an "insertion" attack, and conditions that lend themselves to insertion attacks are the most prevalent vulnerabilities in the intrusion detection systems we tested. An attacker can use insertion attacks to defeat signature analysis, allowing her to slip attacks past an IDS.

To understand why insertion attacks foil signature analysis, it's important to understand how the technique is employed in real ID systems. For the most part, ``signature analysis'' uses pattern-matching algorithms to detect a certain string within a stream of data. For instance, an IDS that tries to detect a PHF attack will look for the string ``phf'' within an HTTP "GET" request, which is itself a longer string that might look something like "GET /cgi-bin/phf?".

The IDS can easily detect the string "phf" in that HTTP request using a simple substring search. However, the problem becomes much more difficult to solve when the attacker can send the same request to a webserver, but force the IDS to see a different string, such as "GET /cgi-bin/pleasedontdetecttthisforme?". The attacker has used an insertion attack to add "leasedontdetectt", "is", and "orme" to the original stream. The IDS can no longer pick out the string "phf" from the stream of data it observes.

Incorrect answers:

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

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

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

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

Obfuscation

Obfuscation refers to the process of concealing something important, valuable, or critical. Cybercriminals use obfuscation to conceal information such as files to be downloaded, sites to be visited, etc.

Unicode invasion

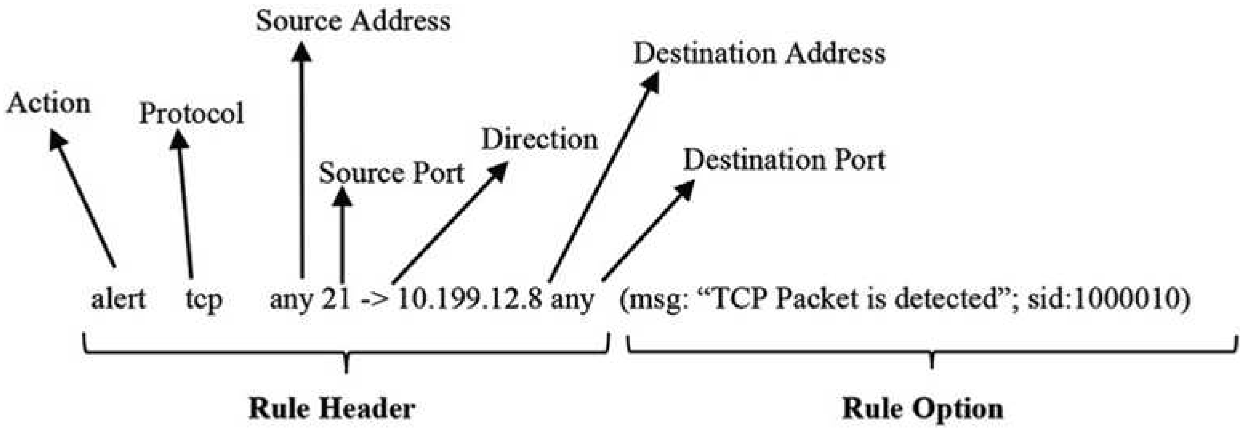
Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.

Question 65:
alert tcp any any -> 10.199.10.3 21 (msg: "FTP on the network!";)

Which system usually uses such a configuration setting?

Firewall IPTable
Router IPTable
FTP Server rule
IDS

Explanation
https://www.snort.org/documents#latest_rule_documents



NOTE: One thing is important to understand: there is no standard for parsers, at least for now. No one will force you, when developing your product, for example, IDS, to create a rule language the same as that of Snort. The question does not specify the manufacturer, although the example clearly hints at the Snort rules, other manufacturers can use the same syntax for anything. In some products, you may not even see the syntax at all cause you may only have access to the graphical user interface. For example, in cloud services, where the stratification of services by levels of abstraction is most clearly visible.

Question 66:
What is a "Collision attack"?
Collision attack on a hash tries to find two inputs producing the same hash value.

Collision attacks break the hash into several parts, with the same bytes in each part to get the private key.
Collision attacks attempt to recover information from a hash.
Collision attacks try to change the hash.

Explanation
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.

NOTE: Yeap, that's all. There is a hash-algorithm with fixed output, and there is an infinite amount of unfixed input; of course, in such a situation, there will be cases when many different inputs give one hash. A simple example: you wrote a letter, calculate its hash, and think that will guarantee its integrity. I intercept it and write my letter and begin to drive in non-printable characters in the message and calculate the hash until the hash of my message and yours will match. How will this help me? Now I can present my message as yours, and that's it - the hash no longer guarantees integrity. Where is this approach used? A digital signature. Or a digital stamp on evidence (such as a USB flash drive or hard drive), and I can intercept it during transportation and changed it. The only problem is that too long a hash will make me search for a collision indefinitely.

Question 67:
Determine the attack by the description:

Determine the attack by the description: The known-plaintext attack used against DES. This attack causes that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key.

Traffic analysis attack
Meet-in-the-middle attack
Man-in-the-middle attack
Replay attack

Explanation
https://en.wikipedia.org/wiki/Meet-in-the-middle_attack

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space–time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations.

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

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.

Replay attack https://en.wikipedia.org/wiki/Replay_attack

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a spoofing attack by IP packet substitution. This is one of the lower-tier versions of a man-in-the-middle attack.

Another way of describing such an attack is: "an attack on a security protocol using replay of messages from a different context into the intended (or original and expected) context, thereby fooling the honest participant(s) into thinking they have successfully completed the protocol run.

Traffic analysis attack https://en.wikipedia.org/wiki/Traffic_analysis

Similar to eavesdropping attacks, traffic analysis attacks are based on what the attacker hears in the network. However, in this type of attack, the attacker does not have to compromise the actual data. The attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behavior patterns.

Traffic analysis method can be used to break the anonymity of anonymous networks, e.g., TORs. There are two methods of traffic-analysis attack, passive and active.

In passive traffic-analysis method, the attacker extracts features from the traffic of a specific flow on one side of the network and looks for those features on the other side of the network.

In active traffic-analysis method, the attacker alters the timings of the packets of a flow according to a specific pattern and looks for that pattern on the other side of the network; therefore, the attacker can link the flows in one side to the other side of the network and break the anonymity of it. It is shown, although timing noise is added to the packets, there are active traffic analysis methods robust against such a noise.

Question 68:
Identify a vulnerability in OpenSSL that allows stealing the information protected under normal conditions by the SSL/TLS encryption used to secure the Internet?

SSL/TLS Renegotiation Vulnerability
Heartbleed Bug
Shellshock
POODLE

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. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.

Incorrect answers:

SSL/TLS Renegotiation Vulnerability

The vulnerability is with the renegotiation feature, which allows one part of an encrypted connection (the one taking place before renegotiation) to be controlled by one party with the other part (the one taking place after renegotiation) to be controlled by another. A MITM attacker can open a connection to an SSL server, send some data, request renegotiation, and, from that point on, continue to forward to the SSL server the data coming from a genuine user. One could argue that this is not a fault in the protocols, but it is certainly a severe usability issue. The protocols do not ensure continuity before and after negotiation.

To make things worse, web servers will combine the data they receive prior to renegotiation (which is coming from an attacker) with the data they receive after renegotiation (which is coming from a victim). This issue is the one affecting the majority of SSL users.

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.

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

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. Bodo Möller, Thai Duong and Krzysztof Kotowicz from the Google Security Team discovered this vulnerability; they disclosed the vulnerability publicly on October 14, 2014 (despite the paper being dated "September 2014"). On December 8, 2014 a variation of the POODLE vulnerability that affected TLS was announced.

Question 69:
The evil hacker Antonio is trying to attack the IoT device. He will use several fake identities to create a strong illusion of traffic congestion, affecting communication between neighbouring nodes and networks. What kind of attack does Antonio perform?

Side-Channel Attack
Forged Malicious Device
Sybil Attack
Exploit Kits

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

The Sybil attack in computer security is an attack wherein a reputation system is subverted by creating multiple identities. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. As of 2012, evidence showed that large-scale Sybil attacks could be carried out in a very cheap and efficient way in extant realistic systems such as BitTorrent Mainline DHT.

An entity on a peer-to-peer network is a piece of software which has access to local resources. An entity advertises itself on the peer-to-peer network by presenting an identity. More than one identity can correspond to a single entity. In other words, the mapping of identities to entities is many to one. Entities in peer-to-peer networks use multiple identities for purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks, the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality, many identities may correspond to the same local entity.

Incorrect answers:

Exploit Kits

An exploit kit is simply a collection of exploits, which is a simple one-in-all tool for managing a variety of exploits altogether. Exploit kits act as a kind of repository and make it easy for users without much technical knowledge to use exploits. Users can add their own exploits to it and use them simultaneously apart from the pre-installed ones.

Side-Channel Attack https://en.wikipedia.org/wiki/Side-channel_attack

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g.

cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

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

Question 70:
John, a penetration tester, decided to conduct SQL injection testing. He enters a huge amount of random data and observes changes in output and security loopholes in web applications. What SQL injection testing technique did John use?

Dynamic Testing.
Static Testing.
Function Testing.
Fuzzing Testing.

Explanation
Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion.

A fuzzer is a program which injects automatically semi-random data into a program/stack and detect bugs.

The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data. New generation fuzzers use genetic algorithms to link injected data and observed impact. Such tools are not public yet.

A fuzzer would try combinations of attacks on:

numbers (signed/unsigned integers/float…)

chars (urls, command-line inputs)

metadata : user-input text (id3 tag)

pure binary sequences

A common approach to fuzzing is to define lists of “known-to-be-dangerous values” (fuzz vectors) for each type, and to inject them or recombinations.

for integers: zero, possibly negative or very big numbers

for chars: escaped, interpretable characters / instructions (ex: For SQL Requests, quotes / commands…)

for binary: random ones

Protocols and file formats imply norms, which are sometimes blurry, very complicated or badly implemented : that’s why developers sometimes mess up in the implementation process (because of time/cost constraints). That’s why it can be interesting to take the opposite approach: take a norm, look at all mandatory features and constraints, and try all of them; forbidden/reserved values, linked parameters, field sizes. That would be conformance testing oriented fuzzing.

Question 71:
Which of the following Nmap options will you use if you want to scan fewer ports than the default?

-p
-T
-sP
-F

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

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Question 72:
Rajesh, a network administrator found several unknown files in the root directory of his FTP server. He was very interested in a binary file named "mfs". Rajesh decided to check the FTP server logs and found that the anonymous user account logged in to the server, uploaded the files and ran the script using a function provided by the FTP server's software. Also, he found that "mfs" file is running as a process and it listening to a network port. What kind of vulnerability must exist to make this attack possible?

File system permissions.
Privilege escalation.
Brute force login.
Directory traversal.

Explanation
File system permissions

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

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

Incorrect answers:

Privilege escalation https://en.wikipedia.org/wiki/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.

Directory traversal https://en.wikipedia.org/wiki/Directory_traversal_attack

A path traversal attack (also known as directory traversal) aims to access files and directories stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control (such as in the case of locked or in-use files on the Microsoft Windows operating system).

This attack is also known as “dot-dot-slash,” “directory traversal,” “directory climbing,” and “backtracking.”

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

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are made by ‘brute force,’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account(s). This is an old attack method, but it's still effective and popular with hackers. Because depending on the password's length and complexity, cracking it can take anywhere from a few seconds to many years.

Question 73:
Michael works as a system administrator. He receives a message that several sites are no longer available. Michael tried to go to the sites by URL, but it didn't work. Then he tried to ping the sites and enter IP addresses in the browser - it worked. What problem could Michael identify?

Traffic is Blocked on UDP Port 69
Traffic is Blocked on UDP Port 53
Traffic is Blocked on UDP Port 88
Traffic is Blocked on UDP Port 56

Explanation
Most likely have an issue with DNS.

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

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

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

The 8 steps in a DNS lookup:

A user types ‘example.com’ into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;

The resolver then queries a DNS root nameserver;

The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;

The resolver then requests the .com TLD;

The TLD server then responds with the IP address of the domain’s nameserver, example.com;

Lastly, the recursive resolver sends a query to the domain’s nameserver;

The IP address for example.com is then returned to the resolver from the nameserver;

The DNS resolver then responds to the web browser with the IP address of the domain requested initially;

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

The browser makes an HTTP request to the IP address;

The server at that IP returns the webpage to be rendered in the browser.

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

Question 74:
Ivan, an evil hacker, conducts an SQLi attack that is based on True/False questions. What type of SQLi does Ivan use?

- **Blind SQLi**
- **Classic SQLi**
- **DMS-specific SQLi**
- **Compound SQLi**

Explanation
https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

Incorrect answers:

Compound SQLi

Compound SQLi is attacks that involve using SQLi alongside cross-site scripting, denial of service, DNS hijacking, or insufficient authentication attacks. Pairing SQLi with other methods of attack gives hackers additional ways to avoid detection and circumvent security systems.

Classic SQLi

Classic SQLi attacks are the most common and simplest form of SQLi. Classic attacks can occur whenever an SQL database allows users to submit an SQL statement. They come in two varieties:

Error-based SQLi, which involves getting a web app to throw an SQL error that gives the attacker either information about the structure of the database or the particular information they're seeking.

UNION-based attacks, which use the SQL UNION operator to determine specifics of the database's structure in order to extract information.

DMS-specific SQLi

Out-of-band SQLi (or DMS-specific SQLi) is a much less common approach to attacking an SQL server. It relies on certain features of an SQL database to be enabled; if those features aren't, the OOB attack won't succeed.

OOB attacks involve submitting a DNS or HTTP query to the SQL server that contains an SQL statement. If successful, the OOB attack can escalate user privileges, transmit database contents, and generally do the same things other forms of SQLi attacks do.

Question 75:
Which of the following web application attack inject the special character elements "Carriage Return" and "Line Feed" into the user’s input to trick the web server, web application, or user into believing that the current object is terminated and a new object has been initiated?

CRLF Injection.
HTML Injection.
Log Injection.
Server-Side JS Injection.

Explanation
CRLF refers to the special character elements "Carriage Return" and "Line Feed." These elements are embedded in HTTP headers and other software code to signify an End of Line (EOL) marker. Many internet protocols, including MIME (e-mail), NNTP (newsgroups) and, more importantly, HTTP, use CRLF sequences to split text streams into discrete elements. Web application developers split HTTP and other headers based on where CRLF is located. Exploits occur when an attacker is able to inject a CRLF sequence into an HTTP stream. By introducing this unexpected CRLF injection, the attacker is able to maliciously exploit CRLF vulnerabilities in order to manipulate the web application's functions.

A more formal name for CRLF injection is Improper Neutralization of CRLF Sequences. Because CRLF injection is frequently used to split HTTP responses, it can also be designated as HTTP Response Splitting or Improper Neutralization of CRLF Sequences in HTTP Headers.

Question 76:
John, a system administrator, is learning how to work with new technology: Docker. He will use it to create a network connection between the container interfaces and its parent host interface. Which of the following network drivers is suitable for John?

Bridge networking.
Macvlan networking.
Host networking.
Overlay networking.

Explanation
https://docs.docker.com/network/macvlan/

Some applications, especially legacy applications or applications which monitor network traffic, expect to be directly connected to the physical network. In this type of situation, you can use the macvlan network driver to assign a MAC address to each container's virtual network interface, making it appear to be a physical network interface directly connected to the physical network. In this case, you need to designate a physical interface on your Docker host to use for the macvlan, as well as the subnet and gateway of the macvlan. You can even isolate your macvlan networks using different physical network interfaces. Keep the following things in mind:

It is very easy to unintentionally damage your network due to IP address exhaustion or to "VLAN spread", which is a situation in which you have an inappropriately large number of unique MAC addresses in your network.

Your networking equipment needs to be able to handle "promiscuous mode", where one physical interface can be assigned multiple MAC addresses.

If your application can work using a bridge (on a single Docker host) or overlay (to communicate across multiple Docker hosts), these solutions may be better in the long term.

Incorrect answers:

Bridge networking https://docs.docker.com/network/bridge/

In terms of Docker, a bridge network uses a software bridge which allows containers connected to the same bridge network to communicate, while providing isolation from containers which are not connected to that bridge network. The Docker bridge driver automatically installs rules in the host machine so that containers on different bridge networks cannot communicate directly with each other.

Host networking https://docs.docker.com/network/host/

If you use the host network mode for a container, that container's network stack is not isolated from the Docker host (the container shares the host's networking namespace), and the container does not get its own IP-address allocated. For instance, if you run a container which binds to port 80 and you use host networking, the container's application is available on port 80 on the host's IP address.

Host mode networking can be useful to optimize performance, and in situations where a container needs to handle a large range of ports, as it does not require network address translation (NAT), and no "userland-proxy" is created for each port.

The host networking driver only works on Linux hosts, and is not supported on Docker Desktop for Mac, Docker Desktop for Windows, or Docker EE for Windows Server.

Overlay networking https://docs.docker.com/network/overlay/

The overlay network driver creates a distributed network among multiple Docker daemon hosts. This network sits on top of (overlays) the host-specific networks, allowing containers connected to it (including swarm service containers) to communicate securely when encryption is enabled. Docker transparently handles routing of each packet to and from the correct Docker daemon host and the correct destination container.

Question 77:
Mark, the network administrator, must allow UDP traffic on the host 10.0.0.3 and Internet traffic in the host 10.0.0.2. In addition to the main task, he needs to allow all FTP traffic to the rest of the network and deny all other traffic. Mark applies his ACL configuration on the router, and everyone has a problem with accessing FTP. In addition, hosts that are allowed access to the Internet cannot connect to it. In accordance with the following configuration, determine what happened on the network?

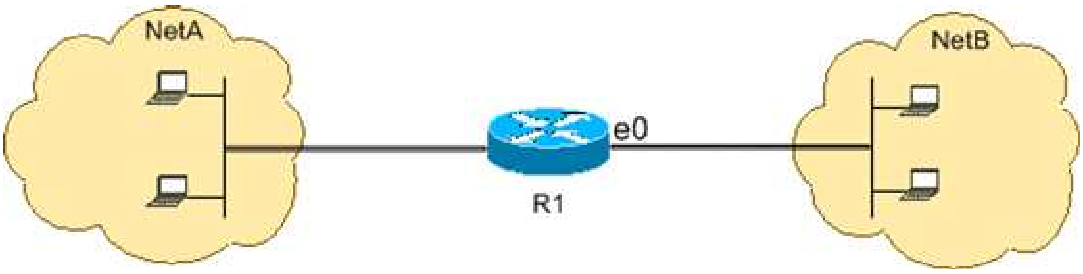
```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

The ACL for FTP must be before the ACL 110.
The ACL 104 needs to be first because is UDP.
The ACL 110 needs to be changed to port 80.
The first ACL is denying all TCP traffic, and the router is ignoring the other ACLs.

Explanation
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.

This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.



FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.

```
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

Question 78:
Which of the following can be designated as "Wireshark for CLI"?

nessus
tcpdump
ethereal
John the Ripper

Explanation
https://www.tcpdump.org/

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

https://www.wireshark.org/

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

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

Incorrect answers:

Nessus https://www.tenable.com/

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);

The presence of default passwords, blank, or weak passwords;

The program has a client-server architecture, which greatly expands the scanning capabilities.

Ethereal - the project was renamed Wireshark in May 2006 due to trademark issues.

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

John the Ripper is a free password cracking software tool.

Question 79:
What is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program?

Concolic testing
Fuzz testing
Security testing
Monkey testing

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

Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.

Incorrect answers:

Concolic testing https://en.wikipedia.org/wiki/Concolic_testing

Concolic testing is a hybrid software verification technique that performs symbolic execution, a classical technique that treats program variables as symbolic variables along a concrete execution path. Symbolic execution is used in conjunction with an automated theorem prover or constaraint solver based on constraint logic programming to generate new concrete inputs (test cases) to maximize code coverage. Its main focus is finding bugs in real-world software rather than demonstrating program correctness.

Monkey testing https://en.wikipedia.org/wiki/Monkey_testing

Monkey testing is a technique where the user tests the application or system by providing random inputs and checking the behavior, or seeing whether the application or system will crash. Monkey testing is usually implemented as random, automated unit tests.

Security testing https://en.wikipedia.org/wiki/Security_testing

Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. Due to the logical limitations of security testing, passing the security testing process is not an indication that no flaws exist or that the system adequately satisfies the security requirements. Typical security requirements may include specific elements of confidentiality, integrity, authentication, availability, authorization and non-repudiation. Actual security requirements tested depend on the security requirements implemented by the system. Security testing as a term has a number of different meanings and can be completed in a number of different ways. As such, a Security Taxonomy helps us to understand these different approaches and meanings by providing a base level to work from.

Question 80:
Which one of the following Google search operators allows restricting results to those from a specific website?

- **[link:]**
- **[inurl:]**
- **[site:] (Correct)**
- **[cache:]**

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

site:

Limit results to those from a specific website.

Incorrect answers:

inurl:

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

link:

Find pages linking to a specific domain or URL. Google killed this operator in 2017, but it does still show some results—they likely aren’t particularly accurate though.

cache:

Returns the most recent cached version of a web page (providing the page is indexed, of course).

Question 81:
Based on the following data, you need to calculate the approximate cost of recovery of the system operation per year:

The cost of a new hard drive is $300; The

chance of a hard drive failure is 1/3; The

recovery specialist earns $10/hour;

Restore the OS and software to the new hard disk - 10 hours;

Restore the database from the last backup to the new hard disk - 4 hours;

Assume the EF = 1 (100%), calculate the SLE, ARO, and ALE.

$146
$440
$960
$295

Explanation
AV (Asset value) = $300 + (14 * $10) = $440 - the cost of a hard drive plus the work of a recovery person, i.e.how much would it take to replace 1 asset? 10 hours for resorting the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.

SLE (Single Loss Expectancy) = AV * EF (Exposure Factor) = $440 * 1 = $440

ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 years is 1/3)

ALE (Annual Loss Expectancy) = SLE * ARO = 0.33 * $440 = $145.2

Question 82:
John needs to choose a firewall that can protect against SQL injection attacks. Which of the following types of firewalls is suitable for this task?

- **Hardware firewall.**
- **Packet firewall.**

Stateful firewall.
Web application firewall.

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

A web application firewall (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

Incorrect answers:

Stateful firewall https://en.wikipedia.org/wiki/Stateful_firewall

A stateful firewall is a network-based firewall that individually tracks sessions of network connections traversing it. Stateful packet inspection also referred to as dynamic packet filtering, is a security feature often used in non-commercial and business networks.

Packet firewall

Packet filtering firewall is a network security technique that is used to control data flow to and from a network. It is a security mechanism that allows the movement of packets across the network and controls their flow on the basis of a set of rules, protocols, IP addresses, and ports.

Hardware Firewalls

Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

Question 83:
Which of the following is the type of violation when an unauthorized individual enters a building following an employee through the employee entrance?

Tailgating.
Pretexting.
Announced.
Reverse Social Engineering.

Explanation
The tailgating attack, also known as “piggybacking,” involves an attacker seeking entry to a restricted area that lacks the proper authentication.

The attacker can simply walk in behind a person who is authorized to access the area. In a typical attack scenario, a person impersonates a delivery driver loaded down with packages and waits until an employee opens their door. The attacker asks that the employee hold the door, bypassing the security measures in place (e.g., electronic access control).

Incorrect answers:

Pretexting

The term pretexting indicates the practice of presenting oneself as someone else to obtain private information. Usually, attackers create a fake identity and use it to manipulate the receipt of information.

Attackers leveraging this specific social engineering technique adopt several identities they have created. This bad habit could expose their operations to the investigations conducted by security experts and law enforcement.

Reverse Social Engineering

A reverse social engineering attack is a person-to-person attack in which an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem.

Question 84:
Which of the following program attack both the boot sector and executable files?

- **Polymorphic virus**
- **Multipartite Virus**
- **Macro virus**
- **Stealth virus**

Explanation
A multipartite virus is a computer virus that can attack both the boot sector and executable files of an infected computer. If you're familiar with cyber threats, you probably know that most computer viruses either attack the boot sector or executable files. However, 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.

According to Wikipedia, the first reported multipartite virus was identified in 1989. Known as Ghostball, it targeted the executable .com files and boot sectors of the infected computer. Since the internet was still in its early years, Ghostball wasn't able to reach many victims. With roughly half of the global population now connected to the internet, multipartite viruses pose a serious threat to businesses and consumers alike.

Incorrect answers:

Stealth Virus

It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of the virus becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

Polymorphic virus https://en.wikipedia.org/wiki/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.

Macro virus https://en.wikipedia.org/wiki/Macro_virus

A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel or word processors such as Microsoft Word. When a macro virus infects a software application, it causes a sequence of actions to begin automatically when the application is opened. Since a macro virus centers on an application and not an operating system, it typically can infect any computer running any operating system.

Macro viruses work by embedding malicious code in the macros associated with documents, spreadsheets, and other data files, causing the malicious programs to run as soon as the documents are opened. Typically, macro malware is transmitted through phishing emails containing malicious attachments. The macro virus spreads quickly as users share infected documents. Once an infected macro is executed, it will typically infect every other document on a user's computer. Some macro viruses cause irregularities in text documents, such as inserting or deleting words. Other macro malware accesses email accounts and sends out copies of infected files to all of the users' contacts, who then open and access these files because they come from trusted sources.

Question 85:
The company "Usual company" asked a cybersecurity specialist to check their perimeter email gateway security. To do this, the specialist creates a specially formatted email message:
From: employee76@usualcompany.com
To: employee34@usualcompany.com
Subject: Test message
Date: 5/8/2021 11:22

He sends this message over the Internet, and a "Usual company " employee receives it. This means that the gateway of this company doesn't prevent _____.

Email Harvesting
Email Masquerading
Email Spoofing
Email Phishing

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

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

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

Incorrect answers:

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

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. When an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, leading to a malware installation, freezing the system as part of a ransomware attack, or revealing sensitive information.

Email Masquerading

A masquerade attack is one where the perpetrator assumes the identity of a fellow network user or co-employee to trick victims into providing user credentials that he/she can then use to gain access to other connected accounts.

Threat actors carry out masquerade attacks by stealing username-and-password combinations via phishing and other means, exploiting security weaknesses or vulnerabilities, or bypassing authentication processes. But the attacker always does so from within the organization.

A masquerade attacker is comparable to a wolf in sheep's clothing. He / She assumes the identity of someone harmless to gain an unsuspecting victim’s trust.

NOTE: Very similar to spoofing, isn't it? Indeed, but here the situation is a little different; the attacker can not only fake the email header, but also, for example, really write on behalf of your friend/boss by gaining access to his/her account. This is a slightly broader concept than spoofing.

Email Harvesting https://en.wikipedia.org/wiki/Email-address_harvesting

Email harvesting or scraping is the process of obtaining lists of email addresses using various methods. Typically these are then used for bulk email or spam.

Question 86:
Rajesh, the system administrator analyzed the IDS logs and noticed that when accessing the external router from the administrator's computer to update the router configuration, IDS registered alerts. What type of an alert is this?

- **False negative**
- **True positve**
- **True negative**
- **False positive**

Explanation
A false positive state is when the IDS identifies an activity as an attack, but the activity is acceptable behavior. A false positive is a false alarm.

Incorrect answers:

False negative

A false negative state is the most serious and dangerous state. This is when the IDS identifies an activity as acceptable when the activity is actually an attack. That is, a false negative is when the IDS misses an attack. This is the most dangerous state since the security professional has no idea that an attack took place.

True positive

A true positive state is when the IDS identifies an activity as an attack, and the activity is actually an attack. A true positive is a successful identification of an attack.

True negative

A true negative state is when the IDS identifies an activity as acceptable behavior, and the activity is actually acceptable. A true negative is successfully ignoring acceptable behavior.

Question 87:
For the company, an important criterion is the immutability of the financial reports sent by the financial director to the accountant. They need to be sure that the accountant received the reports and it hasn't been changed. How can this be achieved?

Use a hash algorithm in the document once CFO approved the financial statements.
Reports can send to the accountant using an exclusive USB for that document.
Use a protected excel file.
Financial reports can send the financial statements twice, one by email and the other delivered in USB and the accountant can compare both.

Explanation
File verification is the process of using an algorithm for verifying the integrity of a computer file. This can be done by comparing two files bit-by-bit, but requires two copies of the same file and may miss systematic corruptions that might occur to both files. A more popular approach is to generate a hash of the copied file and comparing that to the hash of the original file.

File integrity can be compromised, usually referred to as the file becoming corrupted. A file can become corrupted in various ways: faulty storage media, transmission errors, write errors during copying or moving, software bugs, and so on.

Hash-based verification ensures that a file has not been corrupted by comparing its hash value to a previously calculated value. If these values match, the file is presumed to be unmodified. Due to the nature of hash functions, hash collisions may result in false positives, but the likelihood of collisions is often negligible with random corruption.

It is often desirable to verify that a file hasn't been modified in transmission or storage by untrusted parties, including malicious code such as viruses or backdoors. To verify the authenticity, a classical hash function is not enough as they are not designed to be collision resistant; it is computationally trivial for an attacker to cause deliberate hash collisions, meaning that a hash comparison does not detect a malicious change in the file. In cryptography, this attack is called a preimage attack.

For this purpose, cryptographic hash functions are employed often. As long as the hash sums cannot be tampered with — for example, if they are communicated over a secure channel — the files can be presumed to be intact. Alternatively, digital signatures can be employed to assure tamper resistance.

Question 88:
While using your bank's online servicing you notice the following string in the URL bar: http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes. Which type of vulnerability is present on this site?

Web Parameter Tampering
Cookie Tampering
SQL injection
XSS Reflection

Explanation
Correct answer: Web Parameter Tampering

Explanation:

The Web Parameter Tampering attack is based on manipulating parameters exchanged between client and server to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings and is used to increase application functionality and control.

This attack can be performed by a malicious user who wants to exploit the application for their own benefit or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools like Webscarab and Paros proxy are mostly used.

The attack success depends on the integrity and logic validation mechanism errors, and its exploitation can result in other consequences, including XSS, SQL Injection, file inclusion, and path disclosure attacks.

Incorrect answers:

Cookie Tampering: Cookies are files on a user's computer which allow a web application to store information that is subsequently used to identify returning users. Actions by a user or user-specific settings for an application are also stored in cookies. Cookie tampering can be used for attacks such as session hijacking, where cookies with session identification information are stolen or modified by an attacker.

XSS Reflection https://en.wikipedia.org/wiki/Cross-site_scripting#Non-persistent_(reflected)

Cross-site scripting (XSS) is a web application vulnerability that permits an attacker to inject code (typically HTML or JavaScript) into an outside website's contents. When a victim views an infected page on the website, the victim's browser executes the injected code. Consequently, the attacker has bypassed the browser's same-origin policy and can steal private information from a victim associated with the website.

Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off of a web application to the victim's browser.

The script is activated through a link, which sends a request to a website with a vulnerability that enables malicious scripts' execution. The vulnerability is typically a result of incoming requests not being sufficiently sanitized, which allows for the manipulation of a web application's functions and the activation of malicious scripts.

To distribute the malicious link, a perpetrator typically embeds it into an email or third-party website (e.g., in a comment section or social media). The link is embedded inside an anchor text that provokes the user to click on it, which initiates the XSS request to an exploited website, reflecting the attack back to the user.

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.

Question 89:
Ferdinand installs a virtual communication tower between the two authentic endpoints to mislead the victim. What attack does Ferdinand perform?

Aspidistra
Wi-Jacking
Sinkhole
aLTEr

Explanation
aLTEr attack was first published at the 2019 IEEE Symposium on Security & Privacy. It is implemented using a fake eNodeB (the 4G cell tower), acting as Man-in-The-Middle (MiTM): the attacked User Equipment (UE) is persuaded to connect to the network through this equipment, acting as a malicious relay. The researchers have named it “aLTEr attack”.

The vulnerability

The attacker, having access to the encrypted communication of the target UE, takes advantage of the fact that there is no integrity protection on this channel, and manipulates (or aLTErs..) the transmitted information so that the actual communication which arrives at the destination is actually fabricated by the attacker. Since the manipulation is performed on the encrypted channel, the attacker has to alter the communication is such a way so that desired content is produced after decryption. The process of performing this manipulation on the encrypted channel, without having access to the encryption key, is based on the fact that the attacker knows the clear (unencrypted) part of the communication which he intends to manipulate. The mechanism is as elaborated below.

The goal

The goal of the attack is to perform what is known as DNS spoofing. Domain Name Servers (DNS) are the Internet network elements that are responsible for resolving the textual internet addresses (URL) to numerical IP addresses. The attacker’s goal is to alter the IP address of the DNS query issued by the target UE so that the DNS request is routed to a malicious DNS server operated by the attacker. The fake DNS server thus replies maliciously to a request from the target about the IP address of a website to be accessed by the target, ending in the target accessing a malicious site operated by the attacker.

The mechanism

The actual attack is accomplished by the attacker changing the IP address of the DNS server in the query issued by the target device. As described above – the manipulation is performed while the communication is still encrypted. The attacker uses the fact that he or she knows the correct IP address of the legitimate DNS server, so once access is gained to the part in the communication carrying the encrypted true IP address, the attacker knows how to construct a false substitute that will result, once decrypted, in the IP address of the fake DNS server.

Such an attack could be very effective, overcoming the basic security capabilities of LTE and 5G, using the fact that no integrity protection was included.

Question 90:
Which of the following best describes the "white box testing" methodology?

The internal operation of a system is completely known to the tester.
Only the external operation of a system is accessible to the tester.
Only the internal operation of a system is known to the tester.
The internal operation of a system is only partly accessible to the tester.

Explanation
https://en.wikipedia.org/wiki/White-box_testing

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262 processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.

White-box test design techniques include the following code coverage criteria:

Control flow testing

Data flow testing

Branch testing

Statement coverage

Decision coverage

Modified condition/decision coverage

Prime path testing

Path testing

Question 91:
Why is a penetration test considered to be better than a vulnerability scan?

The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Penetration tests are intended to exploit weaknesses in the architecture of your IT network, while a vulnerability scan does not typically involve active exploitation.

A penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.

Vulnerability scans only do host discovery and port scanning by default.

Explanation

Vulnerability scans look for known vulnerabilities in your systems and report potential exposures. Penetration tests are intended to exploit weaknesses in the architecture of your IT network and determine the degree to which a malicious attacker can gain unauthorized access to your assets. A vulnerability scan is typically automated, while a penetration test is a manual test performed by a security professional.

Here's a good analogy: A vulnerability scan is like walking up to a door, checking to see if it is unlocked, and stopping there. A penetration test goes a bit further; it not only checks to see if the door is unlocked, but it also opens the door and walks right in.

Question 92:
Alex, a cybersecurity specialist, received a task from the head to scan open ports. One of the main conditions was to use the most reliable type of TCP scanning. Which of the following types of scanning should Alex use?

Half-open Scan.

TCP Connect/Full Open Scan.)

Xmas Scan.

NULL Scan.

Explanation

TCP Connect/Full Open Scan is one of the most reliable forms of TCP scanning. In TCP Connect scanning, the OS’s TCP connect() system call tries to open a connection to every port of interest on the target machine. If the port is listening, the connect() call will result in a successful connection with the host on that particular port; otherwise, it will return an error message stating that the port is not reachable.

TCP Connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends an SYN packet, which the recipient acknowledges with an SYN+ACK packet. Then, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the scanner sends an RST packet to end the connection.

Incorrect answers:

NULL Scan

The Null Scan is a type of TCP scan that hackers — both ethical and malicious — use to identify listening TCP ports. In the right hands, a Null Scan can help identify potential holes for server hardening, but in the wrong hands, it is a reconnaissance tool. It is a pre-attack probe.

Xmas scan

Nmap Xmas scan was considered a stealthy scan which analyzes responses to Xmas packets to determine the nature of the replying device. Each operating system or network device responds in a different way to Xmas packets revealing local information such as OS (Operating System), port state and more.

Half-open scan

The TCP half-open port scan sometimes referred to as an SYN scan it’s a fast and sneaky scan that tries to find potential open ports on the target computer.

SYN packets request a response from a computer, and an ACK packet is a response. In a typical TCP transaction, there is an SYN, an ACK from the service, and a third ACK confirming the message received.

This scan is fast and hard to detect because it never completes the full TCP 3 way-handshake. The scanner sends an SYN message and just notes the SYN-ACK responses. The scanner doesn’t complete the connection by sending the final ACK: it leaves the target hanging.

Any SYN-ACK responses are possibly open ports. An RST (reset) response means the port is closed, but there is a live computer here. No responses indicate SYN is filtered on the network. An ICMP (or ping) no response also counts as a filtered response.

TCP half-open scans are the default scan in NMAP.

Question 93:
What best describes two-factor authentication for a credit card (using a card and pin)?

Something you have and something you know.
Something you have and something you are.
Something you know and something you are.
Something you are and something you remember.

Explanation
Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows, 2) something the user has, or 3) something the user is.

The possible factors of authentication are:

Something the User Knows:

This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as “Name the town in which you were born.”

Something the User Has:

This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user’s mobile device.

Something the User Is:

This third authentication factor requires the user to authenticate using biometric data. This can include fingerprint scans, facial scans, behavioral biometrics, and more.

For example: In internet security, the most used factors of authentication are:

something the user has (e.g., a bank card) and **something the user knows** (e.g., a PIN code). This is two-factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two-Step Verification, or 2FA.

The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

Question 94:
What means the flag "-oX" in a Nmap scan?

- **Output the results in truncated format to the screen.**
- **Run a Xmas scan.**
- **Output the results in XML format to a file.**
- **Run an express scan.**

Explanation
https://nmap.org/book/man-output.html

-oX <filespec> - Requests that XML output be directed to the given filename.

Incorrect answers:

Run an express scan https://nmap.org/book/man-port-specification.html

There is no express scan in Nmap, but there is a fast scan.

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Or we can influence the intensity (and speed) of the scan with the -T flag. https://nmap.org/book/man-performance.html

-T paranoid|sneaky|polite|normal|aggressive|insane

Output the results in truncated format to the screen https://nmap.org/book/man-output.html

-oG <filespec> (grepable output)

It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl.

Run a Xmas scan https://nmap.org/book/man-port-scanning-techniques.html

Xmas scan (-sX)

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

Question 95:
Which of the following characteristics is not true about the Simple Object Access Protocol?

Only compatible with the application protocol HTTP.
Allows for any programming model.
Exchanges data between web services.
Using Extensible Markup Language.

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

SOAP can be used with any application-level protocol: SMTP, FTP, HTTP, HTTPS, etc. However, its interaction with each of these protocols has its own characteristics, which must be defined separately. Most often SOAP is used over HTTP.

SOAP (formerly an acronym for Simple Object Access Protocol) is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to provide extensibility, neutrality, verbosity and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP), although some legacy systems communicate over Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorize, and communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, SOAP allows clients to invoke web services and receive responses independent of language and platforms.

SOAP provides the Messaging Protocol layer of a web services protocol stack for web services. It is an XML-based protocol consisting of three parts:

an envelope, which defines the message structure and how to process it

a set of encoding rules for expressing instances of application-defined datatypes

a convention for representing procedure calls and responses

SOAP has three major characteristics:

extensibility (security and WS-Addressing are among the extensions under development)

neutrality (SOAP can operate over any protocol such as HTTP, SMTP, TCP, UDP)

independence (SOAP allows for any programming model)

As an example of what SOAP procedures can do, an application can send a SOAP request to a server that has web services enabled—such as a real-estate price database—with the parameters for a search. The server then returns a SOAP response (an XML-formatted document with the resulting data), e.g., prices, location, features. Since the generated data comes in a standardized machine-parsable format, the requesting application can then integrate it directly.

Question 96:
Which of the following wireless standard has bandwidth up to 54 Mbit/s and signals in a regulated frequency spectrum around 5 GHz?

802.11g
802.11i
802.11n
802.11a

Explanation
https://en.wikipedia.org/wiki/IEEE_802.11#802.11a_(OFDM_waveform)

802.11a, published in 1999, uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s. It has seen widespread worldwide implementation, particularly within the corporate workspace.

Incorrect answers:

802.11n

802.11n is an amendment that improves upon the previous 802.11 standards; its first draft of certification was published in 2006. The 802.11n standard was retroactively labelled as Wi-Fi 4 by the Wi-Fi Alliance. The standard added support for multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the 5 GHz bands. Support for 5 GHz bands is optional. Its net data rate ranges from 54 Mbit/s to 600 Mbit/s. The IEEE has approved the amendment, and it was published in October 2009. Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput. 802.11g hardware is fully backward compatible with 802.11b hardware, and therefore is encumbered with legacy issues that reduce throughput by ~21% when compared to 802.11a

802.11i https://en.wikipedia.org/wiki/IEEE_802.11i-2004

IEEE 802.11i-2004, or 802.11i for short, is an amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2). The draft standard was ratified on 24 June 2004. This standard specifies security mechanisms for wireless networks, replacing the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, the amendment deprecated broken Wired Equivalent Privacy (WEP), while it was later incorporated into the published IEEE 802.11-2007 standard.

Question 97:
Which of the following cipher is based on factoring the product of two large prime numbers?
SHA-1
RSA

MD5
RC5

Explanation
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

SA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

Incorrect answers:

SHA-1 https://en.wikipedia.org/wiki/SHA-1

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD2, MD4 and MD5 message digest algorithms, but generates a larger hash value (160 bits vs. 128 bits).

MD5 https://en.wikipedia.org/wiki/MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

RC5 https://en.wikipedia.org/wiki/RC5

RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.

Question 98:
Which of the following command will help you launch the Computer Management Console from" Run " windows as a local administrator Windows 7?

- **gpedit.msc**
- **ncpa.cpl**
- **compmgmt.msc**
- **services.msc**

Explanation
https://www.digitalcitizen.life/ways-open-computer-management-windows/

The Run window is quick method to open system tools in Windows. You can also use it to open Computer Management. Press the Win + R keys on your keyboard to open Run, enter the command compmgmt.msc, and then press Enter or OK.

Incorrect answers:

gpedit.msc

gpedit.msc or Group Policy Editor is a configuration manager for Windows which makes it easier to configure Windows settings. Instead of going through Windows Registry, the user can configure different aspects of the Windows operating system through the Group Policy Editor

ncpa.cpl

Opens the Network Connections in Control panel.

ncpa = Network Control Panel Applet, **cpl** = Control Panel

services.msc

Opens Windows Services Manager.

Question 99:
Which of the following does not apply to IPsec?
Work at the Data Link Layer
Encrypts the payloads
Provides authentication.
Use key exchange.

Explanation
IPsec connections include the following steps:

Key exchange: Keys are necessary for encryption; a key is a string of random characters that can be used to "lock" (encrypt) and "unlock" (decrypt) messages. IPsec sets up keys with a key exchange between the connected devices so that each device can decrypt the other device's messages.

Packet headers and trailers: All data sent over a network is broken down into smaller pieces called packets. Packets contain both a payload, the actual data being sent, headers, or information about that data so that computers receiving the packets know what to do with them. IPsec adds several headers to data packets containing authentication and encryption information. IPsec also adds trailers, which go after each packet's payload instead of before.

Authentication: IPsec provides authentication for each packet, like a stamp of authenticity on a collectible item. This ensures that packets are from a trusted source and not an attacker.

Encryption: IPsec encrypts the payloads within each packet and each packet's IP header (unless transport mode is used instead of tunnel mode). This keeps data sent over IPsec secure and private.

Transmission: Encrypted IPsec packets travel across one or more networks to their destination using a transport protocol. At this stage, IPsec traffic differs from regular IP traffic in that it most often uses UDP as its transport protocol rather than TCP. TCP, the Transmission Control Protocol, sets up dedicated connections between devices and ensures that all packets arrive. UDP, the User Datagram Protocol, does not set up these dedicated connections. IPsec uses UDP because this allows IPsec packets to get through firewalls.

Decryption: At the other end of the communication, the packets are decrypted, and applications (e.g., a browser) can now use the delivered data.

NOTE: Although it is more than enough to know that IPSec works higher, on the third layer (Network layer) and mark the wrong option "Work at the Data Link Layer" (second layer).

Question 100:
According to the Payment Card Industry Data Security Standard, when is it necessary to conduct external and internal penetration testing?

- **At least once a year and after any significant upgrade or modification.**
- **At least twice a year or after any significant upgrade or modification.**
- **At least once every three years or after any significant upgrade or modification.**
- **At least once every two years and after any significant upgrade or modification.**

Explanation
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1608548545820

According to clause 11.3 of Payment Card Industry Data Security Standard: "Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)."

Question 101:
What identifies malware by collecting data from protected computers while analyzing it on the provider's infrastructure instead of locally?
Heuristics-based detection
Behavioural-based detection
Cloud-based detection
Real-time protection

Explanation
Cloud-based detection identifies malware by collecting data from protected computers while analyzing it on the provider's infrastructure instead of locally. This is usually done by capturing the relevant details about the file and the context of its execution on the endpoint and providing them to the cloud engine for processing. The local antivirus agent only needs to perform minimal processing. Moreover, the vendor's cloud engine can derive malware characteristics and behavior patterns by correlating data from multiple systems. In contrast, other antivirus components base decisions, mostly on locally observed attributes and behaviors. A cloud-based antivirus engine allows individual users of the tool to benefit from other community members' experiences.

Incorrect answers:

Behavioral-based detection

Behavioral detection observes how the program executes, rather than merely emulating its execution. This approach attempts to identify malware by looking for suspicious behaviors, such as unpacking of malcode, modifying the hosts file, or observing keystrokes. Noticing such actions allows an antivirus tool to detect the presence of previously unseen malware on the protected system. As with heuristics, each of these actions by itself might not be sufficient to classify the program as malware. However, taken together, they could be indicative of a malicious program. The use of behavioral techniques brings antivirus tools closer to host intrusion prevention systems (HIPS), which have traditionally existed as a separate product category.

Heuristics-based detection

Heuristics-based detection aims at generically detecting new malware by statically examining files for suspicious characteristics without an exact signature match. For instance, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. The tool might also emulate running the file to see what it would do if executed, attempting to do this without noticeably slowing down the system. A single suspicious attribute might not be enough to flag the file as malicious. However, several such characteristics might exceed the expected risk threshold, leading the tool to classify the malware file. The biggest downside of heuristics is it can inadvertently flag legitimate files as malicious.

Real-time protection

Real-time protection is a security feature that helps stop malware from being installed on your device. This feature is built into Microsoft Defender, a comprehensive virus and threat detection program that is part of the Windows 10 security system.

Question 102:
You are configuring the connection of a new employee's laptop to join an 802.11 network. The new laptop has the same hardware and software as the laptops of other employees. You used the wireless packet sniffer and found that it shows that the Wireless Access Point (WAR) is not responding to the association requests being sent by the laptop. What can cause this problem?

- **The laptop is configured for the wrong channel.**
- **The laptop cannot see the SSID of the wireless network.**
- **The WAP does not recognize the la[top's MAC address.**
- **The laptop is not configured to use DHCP.**

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

MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don’t want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.

It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.

The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws.

On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.

MAC address filtering adds an extra layer of security that checks the device’s MAC address against a list of agreed addresses. If the client’s address matches one on the router’s list, access is granted; otherwise, it doesn’t join the network.

Question 103:
Which of the following is a logical collection of Internet-connected devices such as computers, smartphones or Internet of things (IoT) devices whose security has been breached and control ceded to a third party?
Spambot
Botnet
Spear Phishing
Rootkit

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

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the words “robot” and “network.” The Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution. Botnets use your devices to scam other people or cause disruptions — all without your consent.

Incorrect answers:

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.

Advanced Persistent Threats https://en.wikipedia.org/wiki/Advanced_persistent_threat

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. APT attacks are initiated to steal data rather than cause damage to the target organization's network.

APT attacks are typically aimed at organizations in national defense, manufacturing,, and the financial industry, as those companies deal with high-value information, including intellectual property, military plans, and other data from governments and enterprise organizations.

Most APT attacks aim to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible. Because a great deal of effort and resources usually go into carrying out APT attacks, hackers typically target high-value targets, such as nation-states and large corporations, with the ultimate goal of stealing information over a long time.

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

Originally, a rootkit was a collection of tools that enabled administrative access to a computer or network. Today, rootkits are associated with malicious software that provides root-level, privileged access to a computer while hiding its existence and actions. Hackers use rootkits to conceal themselves until they decide to execute their malicious malware.

Besides, rootkits can deactivate anti-malware and antivirus software and badly damage user-mode applications. Attackers can also use rootkits to spy on user behavior, launch DDoS attacks, escalate privileges, and steal sensitive data.

The list below explores some of the possible consequences of a rootkit attack:

Sensitive data stolen

Rootkits enable hackers to install additional malicious software that steals sensitive information, like credit card numbers, social security numbers, and user passwords, without being detected.

Malware infection

Attackers use rootkits to install malware on computers and systems without being detected. Rootkits conceal the malicious software from any existing anti-malware or antivirus, often de-activating security software without user knowledge. As a result of deactivated anti-malware and antivirus software, rootkits enable attackers to execute harmful files on infected computers.

File removal

Rootkits grant access to all operating system files and commands. Attackers using rootkits can easily delete Linux or Windows directories, registry keys, and files.

Eavesdropping

Cybercriminals leverage rootkits to exploit unsecured networks and intercept personal user information and communications, such as emails and messages exchanged via chat.

Remote control

Hackers use rootkits to remotely access and change system configurations. Then hackers can change the open TCP ports inside firewalls or change system startup scripts.

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

A spambot is a computer program designed to assist in the sending of spam. Spambots usually create accounts and send spam messages with them. Web hosts and website operators have responded by banning spammers, leading to an ongoing struggle between them and spammers in which spammers find new ways to evade the bans and anti-spam programs, and hosts counteract these methods.

Question 104:
After several unsuccessful attempts to extract cryptography keys using software methods, Mark is thinking about trying another code-breaking methodology. Which of the following will best suit Mark based on his unsuccessful attempts?

- **Frequency Analysis.**
- **Trickery and Deceit.**
- **Brute-Force.**
- **One-Time Pad.**

Explanation
Trickery and Deceit – it involves the use of social engineering techniques to extract cryptography keys

Brute-Force – cryptography keys are discovered by trying every possible combination

One-Time Pad – a one-time pad contains many non-repeating groups of letters or number keys, which are chosen randomly

Frequency Analysis – It is the study of the frequency or letters or groups of letters in a cipher text. It works on the fact that, in any given stretch of written language, certain letters and combination of letters occur with varying frequencies.

Question 105:
What is meant by a "rubber-hose" attack in cryptography?

Extraction of cryptographic secrets through coercion or torture.
A backdoor is placed into a cryptographic algorithm by its creator.
Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plain text.

Explanation
https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis

A powerful and often the most effective cryptanalysis method in which the attack is directed at the most vulnerable link in the cryptosystem - the person. In this attack, the cryptanalyst uses blackmail, threats, torture, extortion, bribery, etc. This method's main advantage is the decryption time's fundamental independence from the volume of secret information, the length of the key, and the cipher's mathematical strength.

The method can reduce the time to guess a password, for example, for AES, to an acceptable level; however, it requires special authorization from the relevant regulatory authorities. Therefore, it is outside the scope of this course and is not considered in its practical part. (Pss, it's a joke, ok? ^_^)

Question 106:
The firewall prevents packets from entering the organization through certain ports and applications. What does this firewall check?

- **Presentation layer headers and the session layer port numbers.**

Application layer port numbers and the transport layer headers.
Application layer headers and transport layer port numbers.
Network layer headers and the session layer port numbers.

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

The Transport layer provides data segmentation and the control necessary to reassemble these pieces into the various communication streams. Its primary responsibilities to accomplish this are:

Tracking the individual communication between applications on the source and destination hosts;

Segmenting data and managing each piece;

Reassembling the segments into streams of application data

Identifying the different applications.

To pass data streams to the proper applications, the Transport layer must identify the target application. To accomplish this, the Transport layer assigns an application an identifier. The TCP/IP protocols call this identifier a port number. Each software process that needs to access the network is assigned a port number unique in that host. This port number is used in the transport layer header to indicate which application that piece of data is associated with. The Transport layer is the link between the Application layer and the lower layer responsible for network transmission.

https://en.wikipedia.org/wiki/Port_(computer_networking)

Port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number. The most common transport protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

NOTE: A question on a similar topic may occur in your exam, so I decided to answer this question by eliminating deliberately incorrect options. Although, I was probably should intend to answer by listing what the firewalls check. It's just easier and more understandable. The easiest way to filter is to close the port; ports are the essence of the transport layer - the issue is resolved.

But there is a problem here - application layer headers. Some application layer protocols have headers, and some don’t. The OSI model does not specify that they need headers, and if there’s no need to carry control information separate from the payload, they don’t have to have headers.

Probably the creator of a similar question was mistaken in the way the Application Firewall works.

Question 107:
Which of the following requires establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers?

SOX
DMCA

HIPAA
PCI-DSS

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

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act[1][2]) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

The act consists of five titles. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions **and national identifiers for providers, health insurance plans, and employers**.

Title III sets guidelines for pre-tax medical spending accounts.

Title IV sets guidelines for group health plans, and Title V governs company-owned life insurance policies.

Incorrect answers:

SOX https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

The Sarbanes–Oxley Act of 2002, also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. A number of provisions of the Act also apply to privately held companies, such as the willful destruction of evidence to impede a federal investigation.

DMCA https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act

The Digital Millennium Copyright Act (DMCA) is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet. Passed on October 12, 1998, by a unanimous vote in the United States Senate and signed into law by President Bill Clinton on October 28, 1998, the DMCA amended Title 17 of the United States Code to extend the reach of copyright, while limiting the liability of the providers of online services for copyright infringement by their users.

PCI-DSS https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

Question 108:
Identify Bluetooth attck techniques that is used in to send messages to users without the recipient's consent, for example for guerrilla marketing campaigns?

Bluejacking
Bluesnarfing
Bluesmacking
Bluebugging

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

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

Incorrect answers:

Bluesmacking

Bluesmack is a cyber attack done on bluetooth enabled devices. The attack uses L2CAP (Logic Link Control And Adaptation Protocol) layer to transfer an oversized packet to the Bluetooth enabled devices, resulting in the Denial of Service (DoS) attack.

The attack can be performed in a very limited range, usually around 10 meters for the smartphones. For laptops, it can reach up to the 100 meters with powerful transmitters.

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

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

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

Bluebugging is a form of Bluetooth attack often caused by a lack of awareness. It was developed after the onset of bluejacking and bluesnarfing. Similar to bluesnarfing, bluebugging accesses and uses all phone featuresbut is limited by the transmitting power of class 2 Bluetooth radios, normally capping its range at 10–15 meters.

Question 109:
Which of the following layers in IoT architecture helps bridge the gap between two endpoints, such as a device and a client, and carries out message routing, message identification, and subscribing?

Middleware.
Access Gateway.
Edge Technology.
Internet.

Explanation
https://www.jigsawacademy.com/4-layers-of-the-internet-of-things/

https://www.globalsign.com/en/blog/what-is-an-iot-gateway-device

The first layer of the Internet of Things consists of Sensor-connected IOT devices:

These are the small, memory-constrained, often battery-operated electronics devices with onboard sensors and actuators. These could either function as standalone sensing devices or be embedded as part of a bigger machinery for sensing and control. Three main capabilities of a typical IOT device are:

being able to sense and record data

being able to perform light computing and finally

being able to connect to a network and communicate the data

Examples of these include fitness trackers, agricultural soil moisture sensors, medical sensors for measuring blood glucose levels and more. There are a huge number of startups and established companies competing to come up with newer and newer sensors, actuators and devices.

The second layer consists of IOT gateway devices:

The various IOT devices of layer 1 need to be connected to the internet via a more powerful computing device called the IOT gateway which primarily acts like a networking device. So, similar to how a WiFi router helps us connect many laptops, phones and tablets to the internet at home, the IOT gateway aggregates data from numerous sensing devices and relays it to the cloud.

These gateways are critical components of the IOT ecosystem. Typically, IOT gateways are equipped with multiple communication capabilities (like Bluetooth, Zigbee, LoRa WAN, Sub-GHz proprietary protocols) to talk to the IOT devices on one end and a connection to the IP (Internet) based network on the other side (over WiFi, Ethernet or Cellular link).

The Third layer of IOT is the Cloud:

All the sensor data relayed by IOT gateways is stored on cloud hosted servers. These servers accept, store and process data for analysis and decision making. This layer also enables creation of live dashboards which decision makers can monitor and take proactive data driven decisions. Today, almost all cloud computing companies have custom service offerings for IOT solutions.

The forth layer is IOT Analytics:

This is where the magic happens and the collected raw data is converted into actionable business insights, which can help improve business operations, efficiency or even predict future events like machine failure. This layer employs different data science and analytics techniques including machine learning algorithms to make sense of the data and enable corrective action.

Question 110:
Session splicing is an IDS evasion technique that exploits how some IDSs do not reconstruct sessions before performing pattern matching on the data. The idea behind session splicing is to split data between several packets, ensuring that no single packet matches any patterns within an IDS signature. Which tool can be used to perform session splicing attacks?

Hydra
tcpsplice
Whisker
Burp

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

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

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

One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

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

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

Incorrect answers:

tcpsplice https://github.com/the-tcpdump-group/tcpslice

A tool for extracting portions of packet trace files generated using tcpdump's -w flag. https://www.tcpdump.org/

Burp https://portswigger.net/burp

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger.

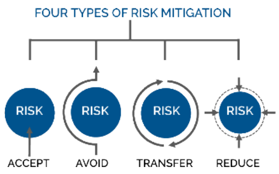
Hydra https://en.wikipedia.org/wiki/Hydra_(software)

Hydra is a parallelized network logon cracker built in various operating systems like Kali Linux, Parrot and other major penetration testing environments. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination. Hydra is commonly used by penetration testers together with a set of programmes like crunch, cupp etc, which are used to generate wordlists. Hydra is then used to test the attacks using the wordlists that these programmes created.

Question 111:
Your company has a risk assessment, and according to its results, the risk of a breach in the main company application is 40%. Your cybersecurity department has made changes to the application and requested a re-assessment of the risks. The assessment showed that the risk fell to 12%, with a risk threshold of 20%. Which of the following options would be the best from a business point of view?

Introduce more controls to bring risk to 0%.
Limit the risk.
Accept the risk.
Avoid the risk.

Explanation
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.



Risk Acceptance

Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Risk Avoidance

Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It’s important to note that risk avoidance is usually the most expensive of all risk mitigation options.

Risk Limitation

Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company’s exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

Risk Transference

Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

NOTE: On my own, I would like to add. It is possible to create absolute protection (0% risk), but with an increase in protection, the system's complexity also grows (and monetary costs, of course). At some point, you can get a complete absence of risks and clients. So you have to compromise and take some risks. This is a profound and interesting topic.

Question 112:
What actions should you take if you find that the company that hired you is involved with human trafficking?

- **Copy the information to removable media and keep it in case you need it.**
- **Stop work and contact the proper legal authorities.**
- **Ignore the information and continue the assessment until the work is done.**
- **Confront the customer and ask her about this.**

Explanation
I think this question is not needed in an explanation, but a question on this topic may occur in your exam, so you need to know how to answer it.

Question 113:
Viktor, the white hat hacker, conducts a security audit. He gains control over a user account and tries to access another account's sensitive information and files. How can he do this?

Fingerprinting
Shoulder-Surfing
Privilege Escalation
Port Scanning

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

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Most computer systems are designed for use with multiple user accounts, each of which has abilities known as privileges. Common privileges include viewing and editing files, or modifying system files.

Privilege escalation means a user receives privileges they are not entitled to. These privileges can be used to delete files, view private information, or install unwanted programs such as viruses. It usually occurs when a system has a bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used. Privilege escalation occurs in two forms:

Vertical privilege escalation, also known as privilege elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications (e.g. Internet Banking users can access site administrative functions or the password for a smartphone can be bypassed.)

Horizontal privilege escalation, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B)

Incorrect answers:

Port Scanning

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. This scanning process can’t occur without identifying a list of active hosts and mapping those hosts to their IP addresses. After a thorough network scan is complete and a host list is compiled, a proper port scan can occur. The organization of IP addresses, hosts, and ports allows the scanner to properly identify open or vulnerable server locations to diagnose security levels.

Fingerprint https://en.wikipedia.org/wiki/Fingerprint_(computing)

A fingerprinting algorithm is a procedure that maps an arbitrarily large data item (such as a computer file) to a much shorter bit string, its fingerprint, that uniquely identifies the original data for all practical purposes just as human fingerprints uniquely identify people for practical purposes. This fingerprint may be used for data deduplication purposes. This is also referred to as file fingerprinting, data fingerprinting, or structured data fingerprinting. Fingerprints are typically used to avoid the comparison and transmission of bulky data. For instance, a web browser or proxy server can efficiently check whether a remote file has been modified, by fetching only its fingerprint and comparing it with that of the previously fetched copy.

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

In computer security, 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 114:
The evil hacker Ivan has installed a remote access Trojan on a host. He wants to be sure that when a victim attempts to go to "www.site.com" that the user is directed to a phishing site. Which file should Ivan change in this case?

Boot.ini
Sudoers
Hosts
Networks

Explanation
https://en.wikipedia.org/wiki/Hosts_(file)

A hosts file is a computer system file that maps human-friendly hostnames (domain names) to their IP address. It uses IP address in IPv4 or IPv6 format to resolve the hostname, and the browser can quickly connect to the hosting server.

While the DNS remains the standard domain name resolution service over the internet, the hosts file overrides the DNS servers. Therefore, you can use the hosts file for various reasons, including redirecting or blocking websites, creating local domains, and sites shortcuts, among other purposes.

Editing Hosts File to Block a website

To block any site from hosts file, you only need to map the hostname to the localhost IP (127.0.0.1) or a full zeros IP address (0.0.0.0) followed by the site's domain name.

Re-directing a Website Using Hosts File

You can also redirect the website to a particular domain. For example, you may edit the hosts file such that whenever a user tries to access Twitter, they are redirected to the company’s site or any other website.

Create Shortcuts for Websites or Intranet Services

You can also modify Windows hosts file to create shortcuts for public or internal sites or web services.

Testing Network / Web Servers

When you are running a web development server on your local network, it will be safe to test its functionality before publishing it live.

Content Filtering and Ads Blocking

You can block Ad networks or unwanted sites by mapping the site to the localhost IP (127.0.0.1).

This will point back to your own PC blocking access to known malicious or Ads sites.

Adding Websites to Hosts File to Improve Browsing Speed

Add a site to the hosts file can increase the browsing speed. This is simply because the computer doesn’t need to query DNS server for IP and waste time waiting for a response.

Preventing Malicious Attacks

The hosts file can be a target for malicious attack. Attackers can use viruses, PUPs and malware to modify the hosts file, redirecting you to malicious sites or hijack your sites.

Incorrect answers:

Sudoers

The /etc/sudoers file controls who can run what commands as what users on what machines and can also control special things such as whether you need a password for particular commands. The file is composed of aliases (basically variables) and user specifications (which control who can run what).

Boot.ini https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/overview-of-the-boot-ini-file

The Boot.ini file is a text file that contains the boot options for computers with BIOS firmware running NT-based operating system prior to Windows Vista. It is located at the root of the system partition, typically c:\Boot.ini.

Networks

Just as with a host's IP address, you should sometimes use a symbolic name for network numbers, too. Therefore, the hosts file has a companion called networks that maps network names to network numbers, and vice versa.

Question 115:
Ivan, an evil hacker, is preparing to attack the network of a financial company. To do this, he wants to collect information about the operating systems used on the company's computers. Which of the following techniques will Ivan use to achieve the desired result?

UDP Scanning.
Banner Grabbing.
SSDP Scanning.
IDLE/IPID Scanning.

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

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

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

Incorrect answers:

IDLE/IPID Scanning https://en.wikipedia.org/wiki/Idle_scan

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

SSDP Scanning https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet protocol suite for advertisement and discovery of network services and presence information. It accomplishes this without the assistance of server-based configuration mechanisms, such as Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS), and without special static configuration of a network host. SSDP is the basis of the discovery protocol of Universal Plug and Play (UPnP) and is intended for use in residential or small office environments. It was formally described in an Internet Engineering Task Force (IETF) Internet-Draft by Microsoft and Hewlett-Packard in 1999. Although the IETF proposal has since expired (April, 2000), SSDP was incorporated into the UPnP protocol stack, and a description of the final implementation is included in UPnP standards documents.

UDP Scanning

UDP scans, like TCP scans, send a UDP packet to various ports on the target host and evaluate the response packets to determine the availability of the service on the host. As with TCP scans, receiving a response packet indicates that the port is open.

Question 116:
Which of the following option is a security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

Spanning tree
Port security
DHCP relay
DAI

Explanation
Dynamic ARP inspection (DAI) protects switching devices against Address Resolution Protocol (ARP) packet spoofing (also known as ARP poisoning or ARP cache poisoning).

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

Incorrect answers:

Port security

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.

You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

Dynamic locking. You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

NOTE: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

Static locking. You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

DHCP relay

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect supported Juniper devices against attacks including spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation.

In a common scenario, various hosts are connected to the network via untrusted access interfaces on the switch, and these hosts request and are assigned IP addresses from the DHCP server. Bad actors can spoof DHCP requests using forged network addresses, however, to gain an improper connection to the network.

Spanning tree https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include backup links providing fault tolerance if an active link fails.

As the name suggests, STP creates a spanning tree that characterizes the relationship of nodes within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Question 117:
Michael, a technical specialist, discovered that the laptop of one of the employees connecting to a wireless point couldn't access the Internet, but at the same time, it can transfer files locally. He checked the IP address and the default gateway. They are both on 192.168.1.0/24. Which of the following caused the problem?
The laptop isn't using a private IP address.
The laptop and the gateway are not on the same network.
The laptop is using an invalid IP address.
The gateway is not routing to a public IP address.

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

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

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

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

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

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

Mediation servers like IRC, Usenet, SMTP and Proxy server

Network address translation (NAT)

Tunneling protocol

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

Question 118:
You have been assigned the task of defending the company from network sniffing. Which of the following is the best option for this task?

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

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

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

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

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

Question 119:
Let's assume that you decided to use PKI to protect the email you will send. At what layer of the OSI model will this message be encrypted and decrypted?

Application layer.
Session layer.
Transport layer.
Presentation layer.

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

In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.

Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

Question 120:
Which of the following UDP ports is usually used by Network Time Protocol (NTP)?

- **19**
- **123**
- **161**
- **177**

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.

NTP is intended to synchronize all participating computers 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 variable network latency effects. NTP can usually maintain time to within tens of milliseconds over the public Internet and achieve better than one millisecond accuracy in local area networks. 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 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.

Incorrect answers: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

19 - Character Generator Protocol (CHARGEN)

177 - X Display Manager Control Protocol (XDMCP)

161 - Simple Network Management Protocol (SNMP)

Question 121:
Andrew is conducting a penetration test. He is now embarking on sniffing the target network. What is not available for Andrew when sniffing the network?
Identifying operating systems, services, protocols and devices.
Capturing network traffic for further analysis.
Collecting unencrypted information about usernames and passwords.
Modifying and replaying captured network traffic.

Explanation
Identifying operating systems, services, protocols and devices,

Collecting unencrypted information about usernames and passwords,

Capturing network traffic for further analysis

are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

Question 122:
Which of the following methods is best suited to protect confidential information on your laptop which can be stolen while travelling?

- **BIOS password.**
- **Hidden folders.**
- **Full disk encryption.**
- **Password protected files.**

Explanation
https://en.wikipedia.org/wiki/Disk_encryption#Full_disk_encryption

The best solution of all the above options is Full Disk encryption as it provides the highest security.

Full disk encryption has several benefits compared to regular file or folder encryption, or encrypted vaults. The following are some benefits of disk encryption:

Nearly everything including the swap space and the temporary files is encrypted. Encrypting these files is important, as they can reveal important confidential data. With a software implementation, the bootstrapping code cannot be encrypted however. For example, BitLocker Drive Encryption leaves an unencrypted volume to boot from, while the volume containing the operating system is fully encrypted.

With full disk encryption, the decision of which individual files to encrypt is not left up to users' discretion. This is important for situations in which users might not want or might forget to encrypt sensitive files.

Immediate data destruction, such as simply destroying the cryptographic keys (crypto-shredding), renders the contained data useless. However, if security towards future attacks is a concern, purging or physical destruction is advised.

Question 123:
How works the mechanism of a Boot Sector Virus?

Moves the MBR to another location on the Random-access memory and copies itself to the original location of the MBR.
Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
Overwrites the original MBR and only executes the new virus code.
Modifies directory table entries to point to the virus code instead of the actual MBR.

Explanation
https://en.wikipedia.org/wiki/Boot_sector#Boot_Sector_Viruses

Among all the viruses, boot sector viruses are one of the oldest forms of computer viruses. At the time of your PC startup time, it infects the boot sector of floppy disks or the Master Boot Record(MBR). Some also infect the boot sector of the hard disk instead of the MBR. To start the operating system and other bootable programs, the boot sector contains all the files required. Before starting any security program like your antivirus program, the boot sector virus runs to execute malicious code.

When the system is booted from an infected disk, the infected code runs. If the infected code runs then, it will rapidly infect other floppy disks. The boot sector virus uses DOS commands while it infects at a BIOS level.

Because this virus is located on the boot sector of your hard drive and runs before the operating system begins, the boot sector virus can cause a lot of damage. Depending on their aim, each boot sector virus works differently. Adware or malware virus creating is the common and general irritating issues.

Most commonly, Boot sector computer viruses are spread using physical media. After it enters a computer, it modifies or replaces the existing boot code. After that, when a user tries to boot their pcs, the virus will be loaded and run immediately. By phishing, you can also be affected by the boot sector virus. It is also possible to send you an attachment with boot sector virus code to your pcs.

Question 124:
Which of the following flags will trigger Xmas scan?

-sP
-sA
-sV
-sX

Explanation
-sX https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

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

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

Null scan (-sN)

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

FIN scan (-sF)

Sets just the TCP FIN bit.

Xmas scan (-sX)

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

Incorrect answers:

-sP

-sP (Skip port scan). This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the scan. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be run.

-sA

-sA (TCP ACK scan). This scan is never determining open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

-sV

-sV (Version detection). Enables version detection. Alternatively, you can use -A, which enables version detection among other things.

Question 125:
Rajesh, a system administrator, noticed that some clients of his company were victims of DNS Cache Poisoning. They were redirected to a malicious site when they tried to access Rajesh's company site. What is the best recommendation to deal with such a threat?

Customer awareness
Use a multi-factor authentication
Use of security agents on customers' computers.
Use Domain Name System Security Extensions (DNSSEC)

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

Cache poisoning tools are available to help organizations prevent these attacks. The most widely used cache poisoning prevention tool is DNSSEC (Domain Name System Security Extension). It was developed by the Internet Engineering Task Force and provided secure DNS data authentication.

When deployed, computers will be able to confirm if DNS responses are legitimate. It also has the ability to verify that a domain name does not exist at all, which can help prevent man-in-the-middle attacks.

DNSSEC will verify the root domain or sometimes called “signing the root.” When an end-user attempts to access a site, a stub resolver on their computer requests the site's IP address from a recursive name server. After the server requests the record, it will also request the zones DNSEC key. The key will then be used to verify that the IP address record is the same as the authoritative server's record.

Next, the recursive name server would verify that the address record came from the authoritative name server. It would then verify it has been modified and resolves the correct domain source. If there has been a modification to the source, then the recursive name server will not allow the connection to occur to the site.

DNSSEC is becoming more prevalent. Many government institutions and financial organizations are making DNSSEC a requirement, as issuing unsigned zones ignores a DNS weakness and leaves your systems open to various spoofing attacks. Organizations need to consider deploying it to protect their data.