EC-Council CEH - Quiz Questions with Answers

Module 01: Introduction to Ethical Hacking

1.

What is the primary goal of a Denial of Service (DoS) attack?

- **To render a system or network unavailable to legitimate users**
- To gain unauthorized access to a system
- To intercept sensitive data in transit
- To delete or modify data on a targeted system

Correct answer: To render a system or network unavailable to legitimate users

A DoS attack aims to overwhelm the target system's resources, such as bandwidth or processing power, causing it to become unavailable to legitimate users.

A DoS attack would not be used to gain unauthorized access to a system, intercept sensitive data in transit, or delete or modify data on a targeted system.

2.

Under FISMA, federal agencies are required to do which of the following?

Develop, document, and implement an agency-wide information security program

Ensure the proper usage and sharing of digital media copyright

Provide open access to all federal data to the public

Implement credit card transaction security measures

Correct answer: Develop, document, and implement an agency-wide information security program

The Federal Information Security Management Act (FISMA) requires federal agencies to create an overarching information security program that ensures the protection of their information systems. This means that they need to develop, document, and implement an agency-wide information security program.

Ensuring the proper usage and sharing of digital media copyright is related to the objectives of the DMCA. Providing open access to all federal data to the public is not a FISMA requirement, as not all federal data is meant to be public. Implementing credit card transaction security measures is related to PCI DSS standards.

3.

An attacker has just successfully executed a denial-of-service attack against a target. Which attribute of the CIA triad is being compromised in this scenario?

Availability

Integrity

Non-repudiation

Confidentiality

Correct answer: Availability

A denial-of-service attack affects the availability of resources. This means that those attempting to access legitimate resources may not be able to do so.

The CIA triad is made up of confidentiality, integrity, and availability. Non-repudiation is not part of the CIA triad, although it is typically considered to be related. A denial-of-service attack would not impact or compromise integrity and confidentiality.

4.

Which of the following refers to the use of information and communication technologies to gain an advantage over an opponent?

- **Information warfare**
- Information security
- Cybercrime
- Service enumeration

Correct answer: Information warfare

Information warfare, or infowar, refers to the use of information and communication technologies to gain an advantage over an opponent. There are both defensive and offensive types of information warfare.

Information warfare is not necessarily illegal, meaning that it isn't cybercrime. Information security, or infosec, refers to the defense and protection of information systems. Service enumeration means identifying services running on a specific target.

5.

Which stage of the Mandiant Attack Lifecycle concerns the attacker's efforts to maintain their position within a compromised network over a prolonged period?

Maintain Presence

Deliver Malware

Internal Reconnaissance

Complete Mission

Correct answer: Maintain Presence

In the Maintain Presence phase, the attacker makes efforts to ensure their continued access to the target environment. There are numerous techniques to establish persistence, such as using the Windows registry or scheduled tasks to keep malware running.

The Deliver Malware stage is for introducing malicious software to the target. Internal Reconnaissance is when the attacker scouts within the network for more information. Complete Mission denotes the stage where the attacker accomplishes their primary objective.

6.

What is the first stage of the cyber kill chain?

Reconnaissance

Weaponization

Delivery

Installation

Correct answer: Reconnaissance

The cyber kill chain is a commonly used framework in the information security space to outline the structure of an attack. Reconnaissance is the first stage in the cyber kill chain.

Weaponization, delivery, and installation all occur after the reconnaissance stage. The correct order of the cyber kill chain is reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objective.

7.

What do "Blue Teams" primarily focus on in cybersecurity exercises?

Defending and securing IT systems.

Attacking and exploiting vulnerabilities

Analyzing malware and its origin

Training employees on cybersecurity practices

Correct answer: Defending and securing IT systems

Blue Teams are oriented toward defense, with a primary focus on securing systems and thwarting attacks. Most organizations are more likely to have an internal security team performing Blue Team activities than an offensive security team (sometimes referred to as a Red Team).

The other options, while part of the broader cybersecurity landscape, don't define a Blue Team's core mission.

8.

Which of the following best defines Information Security?

The protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

The use of technology to break into systems and networks

The process of finding and reporting vulnerabilities

Ensuring software is free from bugs

Correct answer: The protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

The definition of Information Security is the protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Many different teams within an organization play a part in the organization's information security, from the IT and security staff to the end users.

The other options are all related to information security, but they do not define information security overall.

9.

In the Cyber Kill Chain, which step immediately follows weaponization?

Delivery

Reconnaissance

Installation

Exploitation

Correct answer: Delivery

The Cyber Kill Chain framework consists of the seven stages of a cyberattack. Delivery is the third one, right after weaponization.

The framework is as follows:

1. *Reconnaissance*
2. *Weaponization*
3. *Delivery*
4. *Exploitation*
5. *Installation*
6. *Command and Control*
7. *Actions on Objectives*

10.

How many devices were thought to be compromised as part of Mirai botnet?

Over 100,000

About 50,000

Less than 10,000

One million

Correct answer: Over 100,000

The Mirai botnet infected small, special-purpose devices running on an embedded implementation of Linux. The number of devices thought to have been infected by the Mirai botnet is over 100,000.

It's easy to underestimate the number of systems that are compromised each year. Since 2005, there has not been a year without at least 10 million data records being compromised.

11.

What is the primary motivation behind a hacktivist's actions?

To promote or advance a political or social cause

To find and exploit vulnerabilities for financial gain

To vandalize or deface websites for fun

To improve system security by finding and fixing vulnerabilities

---

Correct answer: To promote or advance a political or social cause

Hacktivists usually use their hacking skills to advance a political or social cause. Denial of service attacks are common tactics used by hacktivists to make their agenda known.

Financial gain is generally the motivation behind a black hat hacker. While hacktivists may deface or vandalize websites, they are usually doing it for a cause and not just for fun. Those doing it for fun could be attributed to script kiddies or vandals. White hat hackers, or ethical hackers, are those who seek to improve the security of systems by finding and fixing vulnerabilities.

12.

Maintaining access within a network is also known as which of the following?

Persistence

Enumeration

Footprinting

Privilege escalation

Correct answer: Persistence

Once an attacker has gained access to a target, they typically want to keep and maintain that access. This is known as persistence.

Enumeration and footprinting both refer to different types of information gathering techniques. Privilege escalation is the act of obtaining administrator privileges.

13.

A man-in-the-middle attack compromises which of the following properties of the CIA triad?

- **Integrity**
- Availability
- Confidentiality
- Non-repudiation

Correct answer: Integrity

During a man-in-the-middle attack, an attacker intercepts traffic along its path, alters it, and sends it to its original destination. The attacker being able to alter it compromises integrity.

The CIA triad includes confidentiality, integrity, and availability. Non-repudiation is not part of the CIA triad, but it is often considered related. Availability would be compromised by something like a denial-of-service attack, while confidentiality would be compromised by an attack, which breaks encryption.

14.

Which of the following best describes a honeypot in cybersecurity?

A system set up to lure and monitor attackers

A device that filters out malicious network traffic

A tool used for encrypting data

Software for scanning network vulnerabilities

Correct answer: A system set up to lure and monitor attackers

A honeypot is designed to attract attackers, acting as a decoy, while also monitoring their activities. The honeypot is a distraction so that the attackers stay away from legitimate systems but also give the owners of the honeypot a window into what type of activity the attackers are performing.

A honeypot would not be used to filter out malicious network traffic, encrypt data, or scan for network vulnerabilities. Firewalls, vulnerability scanners, and other security tools can be used to achieve these goals.

15.

Within the MITRE ATT&CK framework, which describes the "how" of an adversary's objectives, detailing the actions to achieve their goal?

Techniques

Tactics

TTPs

Telemetry

Correct answer: Techniques

In the MITRE ATT&CK framework, Techniques describes how adversaries achieve their objectives set out by the tactics. They detail the actions or methodologies adversaries use.

Tactics describes the behavior or overall objective of the attacker. TTPs is an abbreviation for Tactics, Techniques, and Procedures, which encompasses more than just the how. Telemetry refers to the data collected from remote points.

16.

A security professional has successfully gained unauthorized access to a system to test its vulnerabilities. Which type of ethical hacking activity does this best represent?

Penetration testing

Black-box testing

White-box testing

Gray-box testing

Correct answer: Penetration testing

Penetration testing, also known as pen testing, involves authorized hacking attempts to identify security weaknesses in a system.

Black-box testing involves testing without prior knowledge of the system, white-box testing involves testing with full knowledge of the system, and gray-box testing is a combination of both. Because the question doesn't specify how much information was given, the best answer is penetration testing.

17.

What term is used to describe individuals who primarily use pre-written software to conduct hacks, often without a deep understanding of the underlying principles?

Script kiddies

White hat hackers

Black hat hackers

Grey hat hackers

Correct answer: Script kiddies

Script kiddie is a term used for individuals who primarily use existing hacking tools and scripts (often created by others) to conduct hacks, usually without a deep understanding of the systems they are exploiting. Script kiddies are considered unskilled hackers but still pose a threat because they often do not realize the extent of the damage they can cause with the tools they are utilizing.

White hat hackers (also known as ethical hackers) are professionals who use their skills ethically. Black hat hackers create their tools and scripts for malicious intentions. Grey hat hackers are hackers who may sometimes operate without permission but intend to improve system security.

18.

Which law primarily deals with healthcare information security in the U.S.?

HIPAA

SOX

PCI DSS

FISMA

Correct answer: HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is concerned with healthcare information security in the U.S. Anyone working within the healthcare industry needs to be aware of the laws surrounding HIPAA.

The Sarbanes-Oxley Act (SOX) of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations. Payment Card Industry Data Security Standard (PCI DSS) is an information security standard used to handle credit cards appropriately. The Federal Information Security Management Act (FISMA) is a United States federal law enacted in 2002 that made it a requirement for federal agencies to develop, document, and implement an information security program.

19.

What term is often used to describe a hacker who engages in illegal activity?

Black hat

White hat

Gray hat

Red teamer

Correct answer: Black hat

A black hat hacker is a hacker who engages in potentially illegal activities such as breaking into a computer system.

A white hat hacker is someone who does their work for good and does not engage in any illegal activities. A gray hat hacker is someone who falls in the middle. They are typically hacking for good, but their methods and techniques may not be entirely law abiding. A red teamer is someone who performs red team engagements. A red team engagement is generally considered a specific type of penetration test in which the testers act in an adversarial manner to replicate an actual attacker.

The terms white hat, black hat, and gray hat are becoming less commonly used and replaced by terms such as authorized, unauthorized, and semi-authorized entities. Although EC-Council may still use the original terms, it is important to be aware of the new terminology as well.

20.

Which of the following security principles ensures that only authorized parties can access certain information?

Confidentiality

Integrity

Availability

Non-repudiation

Correct answer: Confidentiality

Confidentiality ensures that information is accessible only to authorized individuals or entities and is protected from unauthorized access or disclosure.

Integrity refers to the accuracy and completeness of data, availability refers to ensuring information is accessible when needed, and non-repudiation prevents someone from denying their actions or transactions.

21.

Which of the following is true regarding finding a vulnerability in a system?

You are expected to disclose the vulnerability responsibly to the appropriate parties

You are expected to use your best judgment on whether to disclose found vulnerabilities

You should disclose the vulnerabilities immediately in a public forum

You should disclose the vulnerability only when there is a reward available for disclosure

---

Correct answer: You are expected to disclose the vulnerability responsibly to the appropriate parties

As part of the code of ethics for the Certified Ethical Hacker, you are expected to disclose a vulnerability to the responsible parties when you come across one.

Responsible disclosure doesn't mean reporting the vulnerability in a public forum but instead, working with your employer, any vendor that may be involved, and any Computer Emergency Response Team (CERT) that has jurisdiction over the finding.

22.

What best defines the primary goal of information assurance?

Ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data and services

Detecting and responding to active cyber attacks in real time

Ensuring data is encrypted during transmission over public networks

Assigning user roles and responsibilities in an organization to grant or deny access

---

Correct answer: Ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data and services

The goal of IA is to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of data and services during usage, processing, storage, and transmission of the information. IA covers various aspects of data protection and service reliability.

Detecting and responding to active cyber attacks in real time refers to the function of intrusion detection and response systems. Ensuring data is encrypted during transmission over public networks is specific to data encryption during transmission rather than IA as a whole. Assigning user roles and responsibilities in an organization to grant or deny access outlines the principle of Role-Based Access Control (RBAC).

23.

In which phase of the Mandiant Attack Lifecycle does the attacker first gain access to the target environment?

Initial Compromise

Deliver Malware

Maintain Presence

Escalate Privileges

Correct answer: Initial Compromise

The Mandiant Attack Lifecycle is an alternative to the Cyber Kill Chain and provides a different perspective on how attackers progress through a system. The Initial Compromise phase signifies the point where the attacker first breaches the target environment.

Deliver Malware involves the actual delivery of malicious software to the target. Maintain Presence ensures the attacker retains their access over time. Escalate Privileges is about the attacker seeking higher levels of access within the environment.

24.

Which regulation pertains to the protection of personal data of EU citizens, even if the processing happens outside the EU?

GDPR

HIPAA

SOX

PCI DSS

Correct answer: GDPR

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy. It has a broad reach, affecting organizations outside the EU that handle EU citizens' data.

HIPAA relates to health information in the U.S. SOX is about financial transparency in the U.S. PCI DSS focuses on credit card security.

25.

Which standard is primarily concerned with credit card data security?

- **PCI DSS**
- HIPAA
- ISO/IEC 27001
- GDPR

Correct answer: PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) specifically deals with credit card data security. Any organization or business that accepts and stores credit card data will need to meet PCI DSS standards.

HIPAA is concerned with the privacy of patient health information. GDPR is a privacy standard used in Europe. ISO/IEC 27001 is an international standard to manage information security.

26.

Which of the following authentication factors falls under the category of "something you are"?

Biometric fingerprint

Password

Smart card

PIN

Correct answer: Biometric fingerprint

Authentication factors are classified into three categories: something you are (e.g., biometric characteristics like a fingerprint or iris), something you know (e.g., password or PIN), and something you have (e.g., smart card or security token). Multi-factor authentication should make use of at least two different types of these categories.

PIN and password are something you know. A smart card is something you have.

27.

When malicious code is triggered and infects the target system, this is known as which stage in the cyber kill chain?

Exploitation

Reconnaissance

Delivery

Weaponization

Correct answer: Exploitation

The exploitation stage of the cyber kill chain occurs after the delivery stage. Once the weapon (in the form of malware) is delivered to the target, it is then triggered, infecting the target system during the exploitation stage.

The reconnaissance stage of the cyber kill chain refers to an attacker choosing their target and gathering information about the target. The delivery stage is when the attacker delivers the weapon to the target system, usually via email, USB, or malicious links. The weaponization stage of the cyber kill chain refers to the attacker choosing or creating the weapon they will use to attack the target.

28.

What is the main focus of the reconnaissance phase in the Cyber Kill Chain?

Gathering information about the target

Delivering malware

Establishing command and control

Installing a backdoor to the system

Correct answer: Gathering information about the target

During the reconnaissance phase of the Cyber Kill Chain, the attacker will be gathering as much information as possible about their target. This is the first stage of the Cyber Kill Chain.

Delivering malware is done in the delivery phase. Establishing command and control is part of the command and control stage. Installation involves installing a backdoor in the system to allow for persistent access.

29.

In the context of information assurance, which principle focuses on ensuring that data remains intact and unaltered from its source?

Integrity

Confidentiality

Authentication

Availability

Correct answer: Integrity

Integrity is about ensuring data remains consistent and unaltered unless modification is required. Confidentiality, integrity, and availability are all part of the CIA triad, a set of attributes for information assurance.

Confidentiality ensures data is kept secret from unauthorized entities. Availability emphasizes that systems and data remain accessible. Authentication validates the identity of a user or system.

30.

What is the primary purpose of Information Security Awareness training?

To educate employees about security risks and how to mitigate them

To introduce new IT policies

To monitor employee behavior

To train IT staff on the latest security tools

Correct answer: To educate employees about security risks and how to mitigate them

The main goal of awareness training is to help employees recognize and handle security threats. Organizations should implement regular security training with their employees to prevent security incidents.

The other options involve different objectives related to security and IT policies, but they are not specific to Information Security Awareness training.

31.

Which of the following is a proactive security control technique designed to detect and mitigate ongoing attacks?

- **Intrusion Detection System (IDS)**
- Role-Based Access Control (RBAC)
- Data Loss Prevention (DLP)
- Password hashing

Correct answer: Intrusion Detection System (IDS)

Intrusion Detection Systems (IDSs) are designed to detect and alert for suspicious or malicious activities in real time or near-real time, making it a proactive security control. There are two different types of IDS: host-based IDS and network-based IDS.

RBAC controls user access based on predefined roles. DLP is used to prevent data breaches by monitoring and controlling data transfers. Password hashing is a technique to secure password data.

32.

In which matrix of the MITRE ATT&CK framework would you find information about cloud-based attack vectors?

Enterprise

Mobile

Pre-ATT&CK

ICS

Correct answer: Enterprise

The Enterprise Matrix of the MITRE ATT&CK covers cloud-based as well as on-premises attacks in the ATT&CK framework. The Enterprise Matrix also contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, and Containers.

The Mobile Matrix is focused on mobile devices. Pre-ATT&CK describes the preparation phase before the attack. The ICS Matrix refers to Industrial Control Systems and wouldn't include information about cloud-based attack vectors.

33.

Which of the following best describes the purpose of the MITRE ATT&CK framework?

A knowledge base of adversary tactics, techniques, and procedures

A tool for penetration testing

A firewall configuration guideline

A software vulnerability database

Correct answer: A knowledge base of adversary tactics, techniques, and procedures

The Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) framework is a knowledge base used to describe the actions adversaries take while operating within a network. Tactics, Techniques, and Procedures are often referred to as TTPs.

The MITRE ATT&CK framework is not a tool for penetration testing (although those who conduct penetration tests should be familiar with the framework), a firewall configuration guide, or a vulnerability database.

34.

What is the primary goal of the Federal Information Security Management Act (FISMA)?

To ensure the security of federal information systems

To protect digital copyrights and intellectual property

To establish requirements for financial reporting by corporations

To secure credit card transactions

Correct answer: To ensure the security of federal information systems

The primary goal of the Federal Information Security Management Act (FISMA) is to ensure the security of federal information systems. This includes standards for categorizing information and information systems, standards for minimum security practices, and guidance for security authorization.

Protecting digital copyrights and intellectual property is the goal of the Digital Millennium Copyright Act (DCMA). Establishing requirements for financial reporting by corporations is the goal of the Sarbanes Oxley Act (SOX). The Payment Card Industry Data Security Standard (PCI DSS) is meant to secure credit card transactions.

35.

What's the primary objective of a Denial of Service (DoS) attack?

Overwhelm a system or service, making it unavailable

Steal confidential information

Gain elevated privileges on a system

Install malware on a user's device

Correct answer: Overwhelm a system or service, making it unavailable

The goal of a Denial of Service (DoS) attack is to overwhelm a system or service, making it unavailable. These types of attacks are often used by hacktivists or groups that do not agree with a particular website and want to bring it offline to send a message.

DoS attacks are not used to steal information, gain elevated privileges on a system, or install malware on a system. Key loggers, spyware, ransomware, and other types of attacks can be used to achieve these goals.

36.

Which law introduced significant reforms to improve financial disclosures from corporations to protect investors?

- **Sarbanes Oxley Act (SOX)**
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)

Correct answer: Sarbanes Oxley Act (SOX)

TheSarbanes Oxley Act (SOX) was enacted in response to a number of major corporate and accounting scandals to protect investors from fraudulent financial reporting by corporations. The key requirements and provisions of SOX are organized into 11 titles, such as Auditor Independence and Corporate Responsibilities.

HIPAA concerns health information privacy. PCI DSS focuses on credit card security. GDPR is about personal data protection.

37.

An attacker has just created a piece of custom malware designed specifically to attack their designated target. What phase of the cyber kill chain would this occur in?

Weaponization

Delivery

Exploitation

Installation

Correct answer: Weaponization

The cyber kill chain, also known as the intrusion kill chain, outlines the structure of a cyber attack. Once an attacker has performed reconnaissance on a target, the next step is weaponization. In the weaponization phase, the attacker determines how to attack the target. In some cases, like in this example, the attacker may create a piece of custom malware specific to the target. In other instances, an attacker may choose to just use a piece of common off-the-shelf (COTS) malware.

After determining the weapon (or malware) in the weaponization phase, the delivery phase of the cyber kill chain refers to the transmission of the weapon to the target via email, websites, USB drives, or other means of transport. During the exploitation phase, weaponized code is triggered, exploiting vulnerable applications or systems. The weapon installs a backdoor on the target's system, allowing persistent access during the installation phase. Exploitation leads to installation in which the attacker is able to install additional software to maintain access to the system.

38.

Which of the following is not a part of the CIA triad?

Acceptance

Confidentiality

Integrity

Availability

Correct answer: Acceptance

Acceptance refers to risk acceptance, which is a risk management approach and not part of the CIA triad.

The CIA triad is a set of three attributes (confidentiality, integrity, and availability) that define security.

39.

Which concept emphasizes ensuring that only authorized parties can access specific data or systems?

Confidentiality

Integrity

Non-repudiation

Availability

Correct answer: Confidentiality

Confidentiality involves taking measures to ensure data is not accessed or disclosed to unauthorized individuals, entities, or processes.

Availability ensures that data and services are accessible when needed. Non-repudiation ensures that a party cannot deny the authenticity of their signature on a document or the sending of a message. Integrity ensures data remains unaltered and trustworthy.

40.

What is the final stage of the Cyber Kill Chain?

Actions on Objectives

Installation

Command & Control

Exploitation

Correct answer: Actions on Objectives

The Cyber Kill Chain, developed by Lockheed Martin, describes the stages of a cyberattack. The final stage is Actions on Objectives, where the adversary performs actions to achieve their goals, such as data exfiltration, data destruction, or establishing a persistent presence.

Installation refers to the stage where malware is installed on the victim's system. Command & Control is when the adversary establishes a command channel to control the compromised system. Exploitation is the stage where vulnerabilities in the system are exploited to gain unauthorized access.

41.

Which law makes it illegal to knowingly access a computer without authorization or exceed authorized access?

Computer Fraud and Abuse Act

Sarbanes-Oxley Act

HIPAA

GDPR

Correct answer: Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) makes it illegal to knowingly access a computer without authorization or exceed authorized access. The CFAA was enacted in 1986, as an amendment to the first federal computer fraud law, to address hacking.

The Sarbanes-Oxley Act is related to financial reporting. HIPAA concerns health information privacy, and the EU General Data Protection Regulation (GDPR) is related to data protection and privacy in the European Union.

42.

At which phase in the Mandiant Attack Lifecycle is the attacker's goal, such as data exfiltration or disruption, achieved?

Complete Mission

Escalate Privileges

Establish Foothold

Deliver Malware

Correct answer: Complete Mission

As the name suggests, the Complete Mission phase is where the attacker's main objective or end-goal is realized. However, it is important to note that most attackers are not one-and-done. Even if they have achieved their main goal, they are likely to revisit the network or target once access is achieved to see what more they can do.

The Escalate Privileges phase is when the attacker is working on gaining higher-level access. Establish Foothold is the phase where the attacker ensures sustained access. The Deliver Malware phase refers to the introduction of malicious software to the target system.

43.

TTPs are a fundamental part of which of the following frameworks?

MITRE ATT&CK

Cyber kill chain

Attack lifecycle

OSSTMM

Correct answer: MITRE ATT&CK

The MITRE ATT&CK framework is a taxonomy of Tactics, Techniques, and Procedures (known as TTPs), which describes specific behaviors of attackers.

The cyber kill chain, Open Source Security Testing Methodology Manual (OSSTMM), and attack lifecycle do not detail TTPs.

44.

You are an ethical hacker who has been hired to find vulnerabilities in a company's infrastructure. To start the process, you are researching the company and trying to find any publicly available information about the targets. What stage of the cyber kill chain are you currently in?

Reconnaissance

Delivery

Actions on objectives

Installation

Correct answer: Reconnaissance

During the reconnaissance stage of the cyber kill chain, an attacker researches, identifies, and selects their targets. The cyber kill chain is a commonly referred to framework in the information security space for describing the structure of an attack.

Delivery is the transmission of a weapon to a target via means such as email, websites, and USB drives. During the actions on objectives stage, the attacker works to achieve the objective of the intrusion, which can include exfiltration of data, destruction of data, or intrusion of another target. During the installation stage, the malware installed on a system creates a backdoor on the target system, allowing persistent access.

45.

In which phase of the cyber kill chain does the attacker gain remote access to an infected system?

Command & Control

Delivery

Exploitation

Installation

Correct answer: Command & Control

The command & control phase refers to the attacker gaining remote access to the infected system. Sometimes, command & control is displayed as C2 or C&C.

Delivery is how you get the weapon (such as malware) into the victim's environment. Exploitation would be when the malware infects the victim's system. Installation refers to when an attacker installs additional software to maintain access to the system.

46.

Which technique is utilized to ensure that transmitted data, even if intercepted, cannot be easily read by unauthorized entities?

Data encryption

Intrusion Detection System (IDS)

Role-Based Access Control (RBAC)

Firewall

Correct answer: Data encryption

Data encryption transforms data into a coded format, making it unreadable to unauthorized users. Encryption helps ensure that even if the data is intercepted, confidentiality is kept intact.

An Intrusion Detection System (IDS) detects potentially harmful activities. RBAC provides access based on roles. Firewalls control incoming and outgoing network traffic.

47.

What is the main purpose of an IDS?

To detect potential security breaches in a system

To detect vulnerabilities

To encrypt data transmissions

To serve as a firewall

Correct answer: To detect potential security breaches in a system

An Intrusion Detection System (IDS) is primarily designed to detect unauthorized activity. This is one step below an Intrusion Prevention System (IPS), which is designed to stop unauthorized activity rather than only alert on it.

An IDS would not be used to detect vulnerabilities, serve as a firewall, or encrypt data.

48.

Which of the following best describes the role of a Certified Ethical Hacker?

To identify vulnerabilities and weaknesses in computer systems and networks to improve their security

To hack into computer systems and networks for personal gain

To steal sensitive information from organizations to sell it on the black market

To disrupt the operations of competitor organizations using cyber attacks

---

Correct answer: To identify vulnerabilities and weaknesses in computer systems and networks to improve their security

A Certified Ethical Hacker is an ethical professional who uses hacking techniques and tools to identify and address security vulnerabilities and weaknesses in systems and networks.

The other options describe unethical and illegal activities, and Certified Ethical Hackers are prohibited from performing these types of activities.

49.

The term *ethical hacker* doesn't always show up in job descriptions. Job tiles that utilize ethical hackers are often under different names. Which of the following is likely not a job title that you would see associated with an ethical hacking role?

Hacktivist

Red teamer

Penetration tester

Security researcher

Correct answer: Hacktivist

Hacktivism is a term that combines hacking and activism. A hacktivist is someone who hacks for a specific cause, typically political or humanitarian in nature. Hacktivists often straddle the line between legal and illegal or ethical and unethical cyber activity. As a result, Hacktivist would not be a title that you would see associated with an ethical hacking role.

Penetration tester, red teamer, and security researcher are all job titles related to ethical hacking. If you see these in a job listing, you can feel relatively confident that the role is an ethical hacking role.

50.

A company has implemented a security measure that requires employees to use a smart card and enter a PIN to access the office building. What type of security control is this an example of?

Multi-factor authentication

Firewall protection

Intrusion Detection System (IDS)

Data encryption

Correct answer: Multi-factor authentication

Multi-Factor Authentication (MFA) requires users to provide at least two different types of authentication factors before granting access. In this case, the smart card is something the user has, and the PIN is something the user knows, combining two factors for enhanced security.

Firewalls, intrusion detection systems, and data encryption are all different types of security controls but would not require employees to use multiple forms of authentication to enter the building.

51.

Which U.S. legislation mandates protecting the privacy of individuals' health information?

HIPAA

SOX

PCI DSS

FISMA

Correct answer: HIPAA

Health Insurance Portability and Accountability Act (HIPAA) is the U.S. legislation that mandates the protection of individuals' health information. HIPAA requires that every provider who does business electronically uses the same health care transactions, code sets, and identifiers.

SOX pertains to financial reporting and corporate governance. PCI DSS is a standard for organizations that handle credit card transactions. FISMA relates to federal information systems.

52.

Which U.S. law focuses on financial institutions and requires them to ensure the security and confidentiality of customer data?

Gramm-Leach-Bliley Act

Payment Card Industry Data Security Standard

General Data Protection Regulation

Federal Information Security Management Act

Correct answer: Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to explain their information-sharing practices to their customers and safeguard sensitive data.

Payment Card Industry Data Security Standard (PCI DSS) relates to credit card transaction data. The General Data Protection Regulation (GDPR) is a European regulation. The Federal Information Security Management Act (FISMA) is about the security of federal information systems.

53.

Why do ethical hackers conduct penetration testing?

To identify vulnerabilities and weaknesses in a system before malicious hackers do

To exploit vulnerabilities for personal gain

To perform unauthorized actions on a live system

To develop new hacking tools

Correct answer: To identify vulnerabilities and weaknesses in a system before malicious hackers do

The main goal of penetration testing is to identify vulnerabilities and weaknesses in a system before malicious hackers do. Ethical hackers will always have explicit permission from the system and network owners before conducting their testing.

Ethical hackers would not exploit vulnerabilities for personal gain or perform unauthorized actions on a live system. These actions would be done by malicious actors. While ethical hackers and malicious actors both develop new hacking tools, this isn't why an ethical hacker would conduct a penetration test.

54.

Which among the following is not a primary pillar of Information Security?

Redundancy

Confidentiality

Integrity

Availability

Correct answer: Redundancy

Although redundancy is not part of the CIA triad, having redundancy in place would likely be used to achieve high availability.

The primary pillars of Information Security are Confidentiality, Integrity, and Availability (often termed the CIA triad).

55.

Attackers who use a large number of tactics, techniques, and procedures (TTPs) to gain access to an environment and remain within that environment for as long as they can are known as which of the following?

APT

Hacktivist

Insider threat

Script kiddie

Correct answer: APT

An Advanced Persistent Threat (APT) is an attacker who uses a large number of Tactics, Techniques, and Procedures (TTPs) to gain access to an environment and remain within that environment for as long as they can without being detected. APTs can remain in place for years undetected, gathering intel.

Hacktivists are attackers who attack with a political cause in mind. An insider threat, also known as a malicious insider, is an employee of an organization who knowingly or unknowingly puts the company's security at risk. Script kiddie is a term often used to describe an inexperienced hacker who uses tools created by others to hack into systems.

56.

An attacker moving from one system to another within the same target environment is known as which of the following according to MITRE ATT&CK?

Lateral movement

Reconnaissance

Privilege escalation

Exfiltration

Correct answer: Lateral movement

Lateral movement refers to an attacker moving from one system to another within the same victim's environment to collect more information or to gather details about the systems or users that could be used elsewhere.

Reconnaissance involves selecting a target or gathering information about a victim. Privilege escalation occurs when an attacker is able to gain higher levels of access, such as administrative access, from a lower level account, such as a standard user account. Exfiltration occurs when data is moved outside of the victim's network.

57.

Which of the following types of tests would require an ethical hacker to have no prior knowledge of the network infrastructure?

Black-box testing

White-box testing

Gray-box testing

Blue-box testing

Correct answer: Black-box testing

Black-box testing requires the ethical hacker to have no prior knowledge of the network infrastructure. The terms black-, white-, and gray-box are falling out of popularity in favor of terms such as authorized, unauthorized, and semi-authorized, but these original terms are still used fairly regularly.

Black-box testing differs from white-box testing where the tester has full knowledge of the infrastructure and grey-box testing where the tester has partial knowledge. Blue-box testing is not a recognized term in ethical hacking.

58.

Which of the following, developed by the security consulting company Mandiant, describes how attackers have operated?

Attack lifecycle

Cyber kill chain

ATT&CK framework

OSSTMM

Correct answer: Attack lifecycle

Mandiant developed and uses the attack lifecycle rather than the theoretical and military-focused cyber kill chain. The attack lifecycle describes how attackers have operated for as long as there have been cyber attackers.

The cyber kill chain was developed by Lockheed Martin. The ATT&CK framework was developed by MITRE, and it outlines the tactics, techniques, and procedures that attackers use. OSSTMM stands for the Open Source Security Testing Methodology Manual.

59.

What distinguishes an ethical hacker from a black hat hacker?

Ethical hackers have permission to break into the systems they test

Ethical hackers use different tools than black hat hackers

Black hat hackers are always more skilled than ethical hackers

Ethical hackers only hack into their own systems

Correct answer: Ethical hackers have permission to break into the systems they test

The main difference between an ethical hacker and a black hat hacker is permission and intent. Ethical hackers have explicit permission to test systems, while black hat hackers do not.

Ethical hackers often use many of the same tools that black hat hackers do and are just as skilled. Ethical hackers do not only hack their own systems but also always have permission before hacking systems belonging to others.

60.

A malicious attacker wants to have a piece of malware installed on a target company's system. The attacker put the malware on 50 USB drives disguised as a video file. The malware will run and log all key strokes on the system as soon as an unsuspecting user clicks to open the "video file." The attacker then scattered the USB drives around the office building of the target company, hoping that an employee will pick one up and plug it into a company computer.

What stage of the cyber kill chain does this scenario fall into?

Delivery

Actions on objectives

Installation

Reconnaissance

Correct answer: Delivery

The cyber kill chain is a commonly referred to framework in the information security space for describing the structure of an attack. The delivery stage is the transmission of a weapon to a target via means such as email, websites, and USB drives.

During the actions on objectives stage, the attacker works to achieve the objective of the intrusion, which can include exfiltration of data, destruction of data, or intrusion of another target. During the reconnaissance stage of the cyber kill chain, an attacker researches, identifies, and selects their target. During the installation stage, the malware installed on a system creates a backdoor on the target system, allowing persistent access.

61.

Which of the following best describes the Persistence stage of the MITRE ATT&CK framework?

The attacker needs to ensure that they have access even after a system is rebooted, so they make sure their remote access program runs when the system is started

The attacker is looking for victims or ways to get into the victim's system

The attacker needs to move from one system to another within the victim's environment to collect additional data

The attacker is collecting data and moves the data outside of the victim's environment to one of their own systems

---

Correct answer: The attacker needs to ensure that they have access even after a system is rebooted, so they make sure their remote access program runs when the system is started

The MITRE ATT&CK framework is a taxonomy of Tactics, Techniques, and Procedures (TTPs). The Persistence stage of the ATT&CK framework describes an attacker ensuring that they have ongoing access even after a system is rebooted or changed. This means having the remote access program start up whenever the system is started up.

An attacker looking for victims or ways to get into the victim's system occurs in the reconnaissance stage. An attacker moving from one system to another within the environment is known as lateral movement. Data being moved outside of the target network to the attacker's system is done in the exfiltration stage.

62.

In the Mandiant Attack Lifecycle, which phase involves the attacker trying to move laterally within the network to access more resources?

Internal Reconnaissance

Initial Compromise

Establish Foothold

Complete Mission

Correct answer: Internal Reconnaissance

The Mandiant Attack Lifecycle is an alternative to the Cyber Kill Chain and provides a different perspective on how attackers progress through a system. In the Internal Reconnaissance phase, the attacker, having gained initial access, looks for more information within the network to find further vulnerable systems or valuable data.

Initial Compromise is about the attacker's first entry point, often leveraging a vulnerability or social engineering. Establish Foothold involves the attacker ensuring they maintain their access. Complete Mission is when the attacker achieves their goal, be it data theft, disruption, etc.

63.

In the cyber kill chain developed by Lockheed Martin, which stage follows directly after exploitation?

Installation

Weaponization

Delivery

Actions on objectives

Correct answer: Installation

The cyber kill chain, also known as the intrusion kill chain, outlines the structure of a cyber attack. According to the cyber kill chain, exploitation leads to installation in which the attacker is able to install additional software to maintain access to the system.

During the weaponization phase, the attacker determines how to attack the target, such as what type of malware they will use. After determining the weapon (or malware) in the weaponization phase, the delivery phase of the cyber kill chain refers to the transmission of the weapon to the target via email, websites, USB drives, or other means of transport. During the actions on objectives phase, the attacker performs the goal that they initially set out to do on the target, such as exfiltrating data.

64.

Which law makes it illegal to circumvent digital rights management (DRM) controls on copyrighted materials?

DMCA

FISMA

SOX

PCI DSS

Correct answer: DMCA

The Digital Millennium Copyright Act (DMCA) was created to address the challenges of copyright for digital goods, including making it illegal to bypass Digital Rights Management (DRM) controls. DMCA implements two 1996 treaties of the World Intellectual Property Organization (WIPO).

FISMA is about securing federal information systems. PCI DSS concerns credit card security. SOX established requirements for financial reporting by corporations.

65.

Which of the following best describes the purpose of ethical hacking?

To discover problems and vulnerabilities before attackers, with the goal of improving security

To make money by hacking into targets legally

To hack with the purpose of making a political or human rights statement

To work for intelligence agencies such as the NSA or CIA to assist in national security

---

Correct answer: To discover problems and vulnerabilities before attackers, with the goal of improving security

To improve the security of an organization, it is necessary to know how real-world attackers are able to get in. The purpose of ethical hacking at its core is about discovering programs and vulnerabilities before attackers do, with the goal of improving the overall security posture of the target.

Although you can make money as an ethical hacker by legally hacking into sites, ethical hacking may also be done without payment by performing tests on vulnerability disclosure programs. There are certainly ethical hackers who work within intelligence agencies like the NSA and CIA, but there are also plenty of ethical hackers who work for private companies or even freelance. Hacking to make a political or human rights statement is known as hacktivism, and it is not always done ethically.

66.

In the context of Information Security Controls, what do preventive controls do?

Stops a potential security incident from occurring

Limit the impact of an incident

Indicates the act of a potential security violation

Restores system operations to normal

Correct answer: Stops a potential security incident from occurring

Preventive controls include security mechanisms, tools, or practices that can deter or stop a potential security incident from occurring. An example of a preventive control would be an Intrusion Prevention System (IPS).

Preventive controls do not limit the impact of an incident, indicate the act of a potential security violation, or restore system operations to normal since their goal is to prevent it from happening entirely.

67.

What is the main purpose of using encryption in information security?

To ensure data confidentiality and protect sensitive information

To detect unauthorized access attempts

To prevent the loss of data during hardware failure

To provide real-time monitoring of network traffic

Correct answer: To ensure data confidentiality and protect sensitive information

Encryption is a technique used to convert plaintext data into a secure and unreadable format called ciphertext. It is primarily used to protect the confidentiality of sensitive information, ensuring that even if unauthorized individuals gain access to the data, they won't be able to decipher it.

The other options describe different aspects of information security, but they wouldn't be achieved using encryption.

68.

Which phase of the Cyber Kill Chain involves the adversary establishing a presence on the network?

Installation

Delivery

Reconnaissance

Exploitation

Correct answer: Installation

The installation phase involves an adversary establishing a foothold on the network, often by installing malware. The installation phase follows the exploitation phase in the Cyber Kill Chain.

The other options represent different phases of the Cyber Kill Chain. Delivery involves transmitting the weaponized bundle. Reconnaissance is about gathering information about the target. Exploitation typically involves leveraging a vulnerability that exists on the target.

69.

Which of the following concepts emphasizes the need to provide access only to the information and resources that are necessary for a user's job function?

Principle of Least Privilege

Multi-factor authentication

Continuous monitoring

Data masking

Correct answer: Principle of Least Privilege

The Principle of Least Privilege suggests giving users the minimum levels of access necessary to complete their tasks. The Principle of Least Privilege is sometimes confused with need to know or separation of duties policies, but these are different security concepts.

Multi-factor authentication requires two or more authentication factors before access is granted. Continuous monitoring emphasizes the need to constantly monitor IT systems to detect security threats. Data masking is a method of creating a similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training.

70.

What security control involves classifying user access based on roles within an organization?

Role-Based Access Control (RBAC)

Two-Factor Authentication (2FA)

Intrusion Prevention System (IPS)

Security Information and Event Management (SIEM)

Correct answer: Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) provides access to resources based on roles in an organization. Limiting the access of users to only the resources that they need for their role is considered security best practice and is part of the defense in depth approach to information security.

2FA is an authentication method requiring two different factors. Intrusion Prevention Systems (IPSs) actively prevent or block detected malicious traffic. SIEMs provide real-time analysis of security alerts.

71.

In which phase of the cyber kill chain is the weapon transmitted to the target system (via email, websites, USB drives, or another means of transport)?

Delivery

Reconnaissance

Exploitation

Installation

Correct answer: Delivery

The cyber kill chain, also known as the intrusion kill chain, was developed by Lockheed Martin. The cyber kill chain outlines the structure of a cyber attack. The delivery phase of the cyber kill chain refers to the transmission of a weapon on the target via email, websites, USB drives, or other means of transport.

The reconnaissance phase includes research, identification, and selection of targets. During the exploitation phase, weaponized code is triggered, exploiting vulnerable applications or systems. The weapon installs a backdoor on the target's system, allowing persistent access during the installation phase.

72.

An attacker has successfully gained access to a target system and is in the process of achieving their goal of this hack: to destroy multiple documents on the target system. What stage of the cyber kill chain is this attacker in?

Actions on objectives

Delivery

Installation

Reconnaissance

Correct answer: Actions on objectives

The cyber kill chain is a commonly referred to framework in the information security space for describing the structure of an attack. During the actions on objectives stage, the attacker works to achieve the objective of the intrusion, which can include exfiltration of data, destruction of data, or intrusion of another target.

During the reconnaissance stage of the cyber kill chain, an attacker researches, identifies, and selects their targets. Delivery is the transmission of a weapon to a target via means such as email, websites, and USB drives. During the installation stage, the malware installed on a system creates a backdoor on the target system, allowing persistent access.

73.

An ethical hacker is often also known as which of the following?

White hat

Black hat

Gray hat

Blue hat

Correct answer: White hat

A white hat hacker is someone who does their work for good and does not engage in any illegal activities.

A black hat hacker is a hacker who engages in potentially illegal activities such as breaking into a computer system. A gray hat hacker is someone who falls in the middle. They are typically hacking for good, but their methods and techniques may not be entirely law abiding. The term blue hat is a fictitious term.

The terms white hat, black hat, and gray hat are becoming less commonly used and replaced by terms such as authorized, unauthorized, and semi-authorized entities. Although EC-Council may still use the original terms, it is important to be aware of the new terminology as well.

74.

What is the principle of least privilege in information security?

Users should be granted the minimum levels of access necessary to complete their job functions

All ports should be left open to ensure accessibility

Everyone should have administrative access

Firewalls should be turned off to improve system performance

Correct answer: Users should be granted the minimum levels of access necessary to complete their job functions

The principle of least privilege suggests that users should be granted the minimum levels of access necessary to complete their job functions. This should be done to improve security wherever possible.

Giving everyone administrative access, leaving ports open, and turning off firewalls all create significant security risks.

75.

Which of the following is the first stage of the attack lifecycle as described by the security consulting company Mandiant?

Initial recon

Internal recon

Initial compromise

Establish foothold

Correct: Initial recon

The security consulting company Mandiant uses the attack lifecycle to describe the process of an attack. It is based on how attackers in the past have operated. The first phase of the attack lifecycle is initial recon. During the initial recon stage, the attacker identifies a victim and potential attack possibilities.

The additional stages of the attack lifecycle that follow the initial recon stage are initial compromise, establish foothold, escalate privileges, internal recon, move laterally, maintain presence, and complete mission.

76.

You are looking for a job as an ethical hacker. However, as you begin your job search, you aren't seeing any job postings with *ethical hacker* as the job title. Which of the following would be the best alternative title to search for to find jobs that focus primarily on ethical hacking?

Penetration tester

SOC analyst

Systems engineer

Security analyst

Correct answer: Penetration tester

Ethical hacking and penetration testing are terms that may be used interchangeably. During a penetration test, an ethical hacker attempts to penetrate a system or network's defenses.

Roles such as SOC analyst, systems engineer, and security analyst may all benefit from having knowledge of ethical hacking but are unlikely to focus primarily on ethical hacking in the way that penetration testing or red teaming does.

77.

Which of the following organizations adapted the military's kill chain concept into the cyber kill chain for the information security (or cybersecurity) space?

Lockheed Martin

Mandiant

MITRE

ATT&CK

Correct answer: Lockheed Martin

A kill chain is a military concept that outlines the structure of an attack. The cyber kill chain is a framework in the cybersecurity space that outlines the structure of a cyber attack. A defense contractor, Lockheed Martin, was the first to adapt the military concept of a kill chain to the cyber kill chain.

The phases of the cyber kill chain include reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objectives. Mandiant, a security consulting company, developed the attack lifecycle, which is different from the cyber kill chain. MITRE created the MITRE ATT&CK framework, which outlines the Techniques, Tactics, and Procedures (TTPs) that describe specific behaviors of an attacker.

78.

Which of the following terms best describes "red teaming"?

A specific type of penetration test where the testers act as adversarial to the organization and the network under test

A test to penetrate the defense of an organization

A test involving key stakeholders to test an organization's ability to respond to a cyber attack

An automated tool for finding vulnerabilities in an organization's systems and network

---

Correct answer: A specific type of penetration test where the testers act as adversarial to the organization and the network under test

A red team engagement, or "red teaming," refers to a specific type of penetration test in which the penetration tester acts as an attacker and in an adversarial manner to the organization and the network of the test.

The idea of penetrating the defences of an organization is the description of a standard penetration test. A tabletop exercise is a test of an organization's ability to respond to a cyber attack. A vulnerability scanner is an automated tool that can help identify common vulnerabilities in an organization's systems and network.

Module 02: Footprinting and Reconnaissance

79.

The Internet Assigned Numbers Authority (IANA) owns all IP addresses at a high level. IANA hands out the IP addresses to Regional Internet Registries (RIR) to then pass out to organizations that fall into their geographical region. Which RIR handles the IP addresses for Africa?

- **AfriNIC**
- ARIN
- APNIC
- RIPE

Correct answer: AfriNIC

AfriNIC is the Regional Internet Registry (RIR) that handles IP addresses for Africa.

ARIN handles IP addresses in the United States, Canada, Antarctica, and parts of the Carribean. APNIC handles Asia, Australia, New Zealand, and neighboring countries. RIPE handles Europe, Russia, Greenland, the Middle East, and parts of Central Asia.

80.

Which type of footprinting does not directly interact with the target system and instead gathers information from publicly available sources?

Passive footprinting

Active footprinting

Aggressive scanning

Direct enumeration

Correct answer: Passive footprinting

Footprinting is always the first step in an attack against any information system. During footprinting, information is gathered about the target. Passive and active are the two types of footprinting. Passive footprinting involves collecting data without interacting with the target directly. This is typically done using public information.

Active footprinting involves directly interacting with the target system, such as pinging the system or port scanning. Aggressive scanning relates to active probing but isn't specifically tied to the process of footprinting. Direct enumeration is more related to understanding the specific services and functions of a system rather than broader footprinting.

81.

Which of the following web services can be used to gather information about a website's technology stack?

BuiltWith

WhoIsHostingThis

Google Trends

Moz

Correct answer: BuiltWith

The web service BuiltWith provides details on the technologies, frameworks, and tools a website is using. Another tool that can be used for gathering information about a website's tech stack is Wappalyzer, a browser plugin, that can be added to Chrome or Firefox.

WhoIsHostingThis tells you where a website is hosted but not its tech stack. Moz focuses on Search Engine Optimization (SEO). Google Trends showcases search trends over time.

82.

Andrea is performing network footprinting and reconnaissance. What could she use traceroute for?

To map out the path data takes from the source to the destination

To find vulnerabilities in the network

To crack network passwords

To perform a denial-of-service attack

Correct Answer: To map out the path data takes from the source to the destination

Traceroute is used to map out the path data packets take from the source (Andrea's system) to the destination (the target system), making it a valuable tool in network footprinting for understanding network topology.

The other options, such as finding vulnerabilities, cracking passwords, or performing a denial-of-service attack, cannot be done using traceroute.

83.

Which advanced search operator for search engines allows an ethical hacker to search for specific file types related to a target domain?

- **filetype:**
- inurl:
- site:
- cache:

Correct answer: filetype:

Valuable information about a target can be gathered by performing Google Hacking, a term used to describe the use of advanced search operators to extract sensitive information. The advanced search operator filetype: lets users search for specific file extensions related to the domain.

The inurl: operator searches for specific text within URLs. The site: operator restricts the search to a specific domain or website. The cache: displays what a page looked like the last time Google visited it.

84.

What purpose could ARIN serve during the reconnaissance phase?

To determine the range of IP addresses associated with a target network

To perform a Denial of Service (DoS) attack on a target network

To infiltrate a target network and gain control over its systems

To modify the configuration of a target network's firewall

Correct answer: To determine the range of IP addresses associated with a target network

The American Registry for Internet Names (ARIN) is the Regional Internet Registry (RIR) for the United States, Canada, Antarctica, and parts of the Carribean. During footprinting and reconnaissance, ARIN can be queried to determine the range of IP addresses associated with a target network.

ARIN cannot be used for performing DoS attacks, infiltrating networks, or modifying firewall configurations.

85.

You want to perform a search for a specific username to see if it is being used on any social media sites. Which tool would best achieve this?

Sherlock

CrossLinked

HTTrack

Rubeus

Correct answer: Sherlock

Sherlock is a tool that is installed by default on ParrotOS. When you provide a list of usernames to Sherlock, the tool will go out and search for those usernames across hundreds of social networks.

CrossLinked is a LinkedIn enumeration tool that can provide a list of employees who work for an organization. HTTrack is a tool for mirroring websites. Rubeus is a tool mainly used to perform Kerberoasting attacks.

86.

Jose wants to see the route a packet takes across the internet to reach its destination. Which tool can Jose use to do this?

Tracert

HTTrack

CrossLinked

Dig

Correct answer: Tracert

The command line tool tracert shows the route (in hops) taken by a packet from one point to another.

HTTrack is a website mirroring tool. CrossLinked is a LinkedIn enumeration tool. The program dig is another command line utility, but it is used for name resolution.

87.

Max is a student studying in Russia and is connected to the internet. Which of the following Regional Internet Registries (RIR) is responsible for the IP addresses in Russia?

RIPE

APNIC

ARIN

LACNIC

Correct answer: RIPE

Réseaux IP Européens Network Coordination Centre (RIPE or RIPE NCC) is responsible for the IP addresses in Europe, Russia, Greenland, the Middle East, and parts of Central Asia.

APNIC is responsible for IP addresses for Asia, Australia, New Zealand, and neighboring countries. ARIN handles the United States, Canada, Antarctica, and parts of the Carribean. LACNIC handles Latin America and parts of the Carribean.

88.

Hoang noticed the line Received: from mailserver1.company.com ([192.168.0.10]) in an email header. What can this information be used for in email footprinting?

It identifies an internal mail server of the sender's organization

It provides the public IP address of the sender

It reveals the content of the email

It specifies the email's encryption method

Correct answer: It identifies an internal mail server of the sender's organization

The line Received: from mailserver1.company.com ([192.168.0.10]) gives details about an internal mail server that processed the email. It would tell Hoang that the internal mail server is mailserver1.company.com.

The IP address displayed is a private IP address, not the public IP address of the sender. The line does not provide information about the contents of the email or the encryption method in use.

89.

Which record type is used to indicate the host that email should be sent to for a specific domain?

MX

NS

CNAME

PTR

Correct answer: MX

MX records are mail exchanger records, which indicate the host that email should be sent from for that domain.

NS records are the IP addresses and FQDNs of the authoritative name servers for that domain. A CNAME is an alias for an FQDN. A PTR record is a pointer from an IP address to an FQDN.

90.

What could an attacker potentially do with the information gathered from email footprinting?

- **Launch targeted phishing attacks**
- Decrypt encrypted files
- Directly access the internal database
- Modify the source code of the email server

Correct Answer: Launch targeted phishing attacks

Information obtained from email footprinting can be used by an attacker to launch targeted phishing attacks. This is because the attackers may be able to see what types of emails the target typically receives, or they can impersonate a contact that the target has interacted with in the past.

The other options are not directly related to the use of information obtained from email footprinting.

91.

What can an ethical hacker determine by using the Time to Live (TTL) value in an ICMP echo request and response?

Approximate distance (in hops) to the target

The type of operating system on the target

Open ports on the target

Subdomains associated with a target domain

Correct answer: Approximate distance (in hops) to the target

The TTL value can be used to estimate the number of hops to a target. Utilities like traceroute and ping use TTL to reach the host or trace a route to that host.

While the type of OS can sometimes be inferred from TTL values and ICMP responses, it's not as direct as the distance. Determining open ports on a target requires port scanning, and finding subdomains associated with a target domain requires domain enumeration techniques.

92.

When performing an investigation into webpages and the technologies used, you can use developer tools on Google Chrome. What is the equivalent to Chrome's developer tools on the Firefox web browser?

Firebug

Firefly

Foxtools

FoxDev

Correct answer: Firebug

Firebug is a tool available on Firefox that allows you to dig into a website and the technologies used. You can look at the Document Object Model (DOM) and all its components. You can also select and inspect different HTML elements in the page.

Firefly, Foxtools, and FoxDev are fictitious names.

93.

What potential risk do geotagged photos on social media platforms pose?

They can reveal the physical locations of individuals or assets

They decrease the image's resolution

They allow direct access to the user's device

They tag the individual's IP address

Correct answer: They can reveal the physical locations of individuals or assets

Geotagged photos contain metadata about where the photo was taken, which can inadvertently reveal sensitive location information.

Geotagging does not present the risk of decreasing the image's resolution, allowing direct access to the user's device, or tagging the individual's IP address.

94.

You are doing reconnaissance on a target company for a red team engagement using OSINT techniques. You'd like to look up public filings associated with the target company, such as their annual and quarterly reports, which show details about the company's finances. Where could you look to find this information?

EDGAR

Domain registrars

Whois

LinkedIn

Correct answer: EDGAR

The Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system is a Securities and Exchange Commission (SEC) database that stores public information about public companies. Using this system, you can look up public filings such as an annual report in Form 10-K or quarterly reports in Form 10-Q.

Domain registrars also have public information about companies and can be used in OSINT, but they don't provide the same type of information (e.g., annual and quarterly reports) as EDGAR. Whois is an internet record listing that identifies who owns a domain and how to contact the domain owner if you need to. LinkedIn is a social networking site primarily used by professionals. LinkedIn is great for OSINT but would not be useful in this particular scenario.

95.

You want to view a company's annual report on EDGAR to get an overview of the business. What is the name given to the annual report on EDGAR?

10-K

10-Q

11-K

17-H

Correct answer: 10-K

The Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system stores all public filings associated with a company. The annual reports, called 10-K, provide an overview of the business.

Quarterly reports on EDGAR are called 10-Qs. An 11-K form provides information about employee stock options and plans. A 17-H form is a risk assessment for brokers and dealers.

96.

In social media footprinting, what can be inferred by analyzing a target's posts, likes, and comments?

Personal interests, locations, and activities

The target's computer specifications

The target’s password

The security configuration of the target's network

Correct answer: Personal interests, locations, and activities

Analyzing posts, likes, and comments can disclose personal information, including interests, location history, and activities. This is because individuals tend to post about places they frequently visit or their favorite hobbies.

The other options are typically not determinable from social media activity analysis.

97.

You want to dump the DNS cache on a Windows system, and you already have access to the command line. Which command should you run?

ipconfig /displaydns

nslookup

ipconfig /showcache

nslookup /dnscache

Correct answer: ipconfig /displaydns

Windows systems cache values, and they can be dumped using the ipconfig /displaydns command.

The nslookup program is a DNS lookup tool but can't be used to dump the cache on a Windows system. Ipconfig /showcache and nslookup /dnscache are not valid commands.

98.

Which DNS record type can be used to store text entries that do not have a specific purpose but can be used for a variety of reasons?

- **TXT**
- MX
- AAAA
- PTR

Correct answer: TXT

A TXT record is a record type that is used to store text entries that don't have a specific purpose but can be used for a variety of reasons. For example, TXT records are a key part of many email authentication methods.

An MX record is used to indicate which host email should be sent to for a specific domain. An AAAA record converts an FQDN to an IPv6 IP address. A PTR record is a pointer from an IP address to an FQDN.

99.

What kind of information can be obtained from a WHOIS lookup?

Information about the owner of a domain name

The contents of a target's database

The number of visitors to a target's website

The passwords of a target's system users

Correct answer: Information about the owner of a domain name

A WHOIS lookup provides information about the owner of a domain name and related IP addresses. WHOIS will query Regional Internet Registries (RIR) and domain registrars.

WHOIS does not provide database contents, website visitor numbers, or passwords.

100.

What is Google dorking primarily used for in footprinting?

Advanced searching to find specific information about a target

Hacking into Google servers

Sending phishing emails

Decrypting passwords

Correct answer: Advanced searching to find specific information about a target

Google dorking involves using advanced operators in the Google search engine to locate specific information about a target. The Google Hacking DataBase (GHDB) stores and lists many search terms for locating vulnerable files, error messages, and sensitive directories.

Google dorking isn't used to hack Google servers, send phishing emails, or decrypt passwords.