1. Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion,directories, web research, etc. are important sources of information for an ethical hacker. Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

2. Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

3. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.

4. Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

5. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources.

```
nbtstat -a <target_ip_address>
nbtstat -c
net use
```

6.LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

7. set querytype=soa sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain certifiedhacker.com.
In this command, ls -d requests a zone transfer of the specified name server.

8.   Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

9. L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

10. Creating a Share :
Type mkdir /var/www/html/share and press Enter to create a shared folder
Type chmod -R 755 /var/www/html/share and press Enter
Type chown -R www-data:www-data /var/www/html/share and press Enter
Copy the malicious file to the shared location by typing cp /root/Desktop/Test.exe /var/www/html/share and pressing Enter

11. Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

12. A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

13. Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.

14. HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

15. HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

16. Session hijacking can be divided into three broad phases:

Tracking the Connection: The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict

Desynchronizing the Connection: A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)

Injecting the Attacker's Packet: Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

17. njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

18. Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses

19. SwayzCryptor is an encrypter (or “crypter”) that allows users to encrypt their program’s source code.

20. Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose. The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware’s functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

21. Perform a Strings Search using BinText :
Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

22.

DriverView The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.
Driver Reviver Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

23. DNSSEC protects the internet community from forged DNS data by using public key cryptography to digitally sign authoritative zone data when it comes into the system and then validate it at its destination.

When an end user wants to access a website, a stub resolver on the user's computer requests the website's IP address from a recursive name server. After the server requests this record, it also requests the DNSSEC key associated with the zone. This key allows the server to verify that the IP address record it receives is identical to the record on the authoritative name server.

24. Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

25. Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable “back-end” tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

```
        nc -vv www.certifiedhacker.com 80
        GET / HTTP/1.0      press 2 times enter
```

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.

- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

```
telnet www.certifiedHhacker.com 80
```

26. Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery**: Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery**: Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification**: Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery**: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

27. Clickjacking, also known as a “UI redress attack,” occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for the top-level page and routing them to another page, most likely owned by another application, domain, or both.

28. Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.

29. CSRF, also known as a one-click attack, occurs when a hacker instructs a user’s web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks. The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user’s browser to send malicious requests that they did not intend.

30.

- **In-band SQL injection**: An attacker uses the same communication channel to perform the attack and retrieve the results
- **Blind/inferential SQL injection**: An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database
- **Out-of-band SQL injection**: An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results

31. Fragmentation attack: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)

1. **MAC spoofing attack**: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point’s MAC-filtering configuration
2. **Disassociation attack**: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
3. **Deauthentication attack**: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point

4. **Man-in-the-middle attack**: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
5. **Wireless ARP poisoning attack**: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
6. **Rogue access points**: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator

7. **Evil twin**: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
8. **Wi-Jacking attack**: A method used by attackers to gain access to an enormous number of wireless networks

32. WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise.

33. Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.

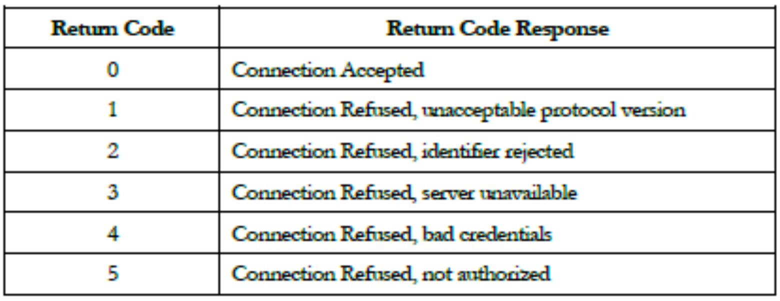
34. MQTT Explorer is a comprehensive MQTT client that provides a structured overview of your MQTT topics and simplifies working with devices/services on your broker.

35. The MQTT protocol establishes a connection between clients through a broker. A CONNECT command is sent to initiate a connection from the client to the broker. After the connection is established, it remains active until a disconnect command is sent from the client. Some of the headers of the CONNECT command are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- Connect Flags: Contains parameters specifying the behavior of the MQTT connection.
- Clean Session: Indicates whether the client wants to establish a persistent connection with the broker or not.
- Client ID: Indicates a unique identifier for each MQTT client connecting to an MQTT broker.

36. The broker sends the Connect Ack packet on receiving a Connect command request from the client. Some of the headers in the Connect Ack packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- Session Present: Indicates the session between the broker and client; Bit 0 is the Connection Ack bit in the session present flag.
- Return Code: The values and responses of the return code are summarized in the table below:



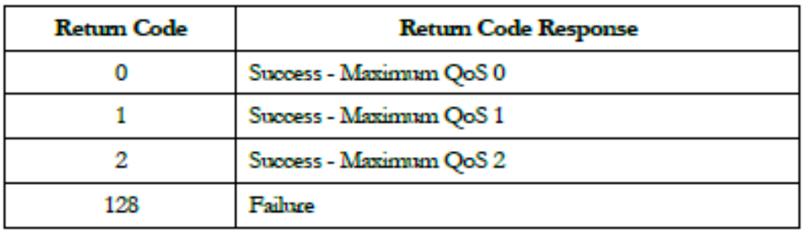
Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, server unavailable
4	Connection Refused, bad credentials
5	Connection Refused, not authorized

To receive a relevant message, a client sends a SUBSCRIBE message to an MQTT broker. Some of the headers in the Subscribe Request packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- Message Identifier: Identifies a message in a message flow between a client and a broker.
- Topic and QoS Level: A subscription is a pair of a topic filter and a QoS level; the topic defines a subject of interest on which the client would like to get messages.
- Payload: Contains a list of subscriptions.

The MQTT broker confirms subscription by sending an acknowledgment back to the client using a SUBACK message. Some of the headers in the Subscribe Acknowledgement packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- Message Identifier: Identifies a message in a message flow between a client and a broker.
- Payload: Contains a list of return codes.
- Return Code: For each Topic/QoS pair received, a return is sent by the MQTT broker in the SUBSCRIBE message; the return code is in line with the QoS level in the case of a success.



Return Code	Return Code Response
0	Success - Maximum QoS 0
1	Success - Maximum QoS 1
2	Success - Maximum QoS 2
128	Failure

After establishing a successful connection with the MQTT broker, the MQTT client can publish messages. The headers in the Publish Message packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- DUP flag: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message.
- QoS: Determines the assurance level of a message.
- Retain Flag: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic.
- Topic Name: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured.
- Message: Contains the actual data to be transmitted.
- Payload: Contains the message that is being published.

37. S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- **Inspecting HTML**: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- **Brute-Forcing URL**: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains**: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search**: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking**: Use advanced Google search operators such as **"inurl"** to search for URLs related to the target S3 buckets

38. Horizontal Privilege Escalation: An unauthorized user tries to access the resources, functions, and other privileges of an authorized user who has similar access permissions
Vertical Privilege Escalation: An unauthorized user tries to access the resources and functions of a user with higher privileges such as application or site administrators

39. MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

40. The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

41. Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key. The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

42. Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis**: A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis**: The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis**: This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis