# Ethical Hacking Task - Theoretical

# Question 1

**There are three methodologies for ethical hacking. Name these methodologies and explain them in your own words.**  
1)Blackbox Penetration Testing:   
The penetration tester will not be provided with any information about the tested subject apart from its address/location/name. This methodology is common when the tested subject is exposed to the internet or a wide range of unauthorized users.  
  
2)Graybox Penetration Testing:   
The penetration tester will be provided with limited information about and credentials for the tested subject.  
  
3)Whitebox Penetration Testing:   
The penetration tester will be provided with all information and credentials about the tested subject, including its source code, network architecture, and administrative access to security controls.

# Question 2

**Name three tools used by ethical hackers and explain each of them.**  
Metlasploit:   
This framework is a collection of ready-to-use exploitation tools that can be integrated and customized to create various payloads to exploit all the latest vulnerabilities. Metasploit’s features for exploitation are called “modules” and are updated regularly with new modules based on the newest releases in the field.

SQLMap:   
It is a open-source tool used for detecting and exploiting various SQLi vulnerabilities. Using pre-defined parameters and automated processes, it can detect vulnerabilities in varios scenarios – includibg in a wide selection of DBMSs and to identify and exploit SQL injection vulnerabilities in web applications.  
The tool is written in Python and can be used on multiple operating systems, including Windows, Linux, and Unix-based OS (MacOS, for example).

NMAP:   
It is a free, open-source network scanner designed to explore endpoints, servers, and services to perform network scans and provide detailed information about the networks and their connected devices and to display a list of active hosts and open ports.  
It provides a wide variety of features to help ethical hackers identify and assess potential attack vectors. This process is called “network scanning or “port scanning”.

# Question 3

**What is network sniffing?**  
Network sniffing, also known as packet sniffing or packet capturing, refers to the practice of intercepting and analyzing network traffic passing through a computer network. It involves capturing packets of data as they traverse the network and inspecting their contents for various purposes, such as network troubleshooting, performance analysis, and security monitoring.

# Question 4

**Give an example of a network sniffing tool and a case in which you, as a future cyber security expert, would use this tool.**  
One example of a popular network sniffing tool is Wireshark. Wireshark is an open-source packet analyzer that allows users to capture and analyze network traffic in real-time.  
  
As a future cybersecurity expert, you might use Wireshark in various scenarios. Here's an example:  
  
Case: Network Intrusion Detection  
Suppose you are responsible for monitoring and securing a corporate network. You receive reports of suspicious network activity and suspect a potential intrusion attempt. In this case, you could use Wireshark to capture and analyze network traffic to identify any malicious activities or anomalies.  
  
Using Wireshark, you would set up a network interface to capture packets and filter the traffic based on specific criteria, such as source IP address, destination IP address, or protocol. You could then analyze the captured packets to identify any indicators of compromise, such as unusual network connections, unauthorized access attempts, or suspicious communication patterns.  
  
Wireshark provides detailed packet-level information, allowing you to examine the contents of each packet, including the headers, payloads, and protocols being used. By analyzing the captured packets, you can gain insights into the nature and extent of the suspected intrusion, enabling you to take appropriate actions to mitigate the threat and secure the network.  
  
It's important to note that using network sniffing tools like Wireshark requires proper authorization and adherence to legal and ethical guidelines. Network sniffing should only be performed within the scope of legitimate security operations and in compliance with applicable laws and regulations.

# Question 5

**There are two testing conditions that must be predefined before hacking begins, according to the client's expectations and the desired results – internal or external testing and protected or fully exposed.  
  
Explain what each of these conditions means and how they may affect hacking:  
  
  
Internal or external testing  
Protected or fully exposed**  
-Internal or external testing: This term refers to whether the tested subjects are exposed to the internet(external) or are in a closed corporate network(internal). This may affect the probability of exploiting vulnerabilities on the subject, since it may be harder to reach internal targets.  
-Protected or fully exposed: This term refers to whether the tested subjects are protected by any security controls, such as firewalls, IDS/IPS, or web application firewalls (WAFs). While these security controls may provide extra protection for the tested subjects, they usually interrupt the hacking process because it is harder to reach the “real” tested subjects.

**How would you choose to test your network and why?**  
When choosing how to test a network, consider the following factors:  
-Goals and objectives: Determine the specific goals of the testing, such as identifying vulnerabilities or assessing overall security posture.  
-Testing scope: Define the scope of the testing, focusing on critical systems or the entire network infrastructure.  
-Resources and expertise: Assess available resources and expertise, either in-house or through external consultants.  
-Compliance and regulatory requirements: Consider any industry-specific compliance or regulatory requirements for testing.  
-Risk tolerance: Understand the organization's risk tolerance level for more aggressive or cautious testing approaches.  
  
Based on these considerations, you can choose methods like vulnerability assessments, penetration testing, social engineering testing, or red team testing. Combining multiple methods provides a comprehensive assessment of the network's security.

# Question 6

**Lockheed Martin created a Cyber Kill Chain model that divided a cyber-attack into seven stages.&nbsp;  
Name these seven stages.**  
1)Reconnaissance  
2)Weaponization  
3)Delivery  
4)Exploitation  
5)Installation  
6)Command and Control  
7)Actions on Objective

**Name two of these stages and describe them in your own words.**  
1)Reconnaissance: Find the target. Attackers choose the target.  
2)Weaponization: Develop a weapon. The weapon is usually malware such a trojan or ransomware whose goal is to exploit the target’s vulnerabilities.

# Question 7

**Google hacking is the practice of using Google as a hacking tool. Name three ways ethical hackers use Google hacking.**  
-Footprinting and Reconnaissance: Ethical hackers can use Google hacking to gather information about a target organization or individual. By leveraging advanced search operators and queries, they can discover exposed sensitive information, such as usernames, passwords, login pages, network devices, or confidential documents. This helps in understanding the target's digital footprint, identifying potential vulnerabilities, and guiding further penetration testing efforts.  
  
-Vulnerability Identification: Google hacking can assist ethical hackers in identifying potential vulnerabilities in web applications, websites, or network infrastructure. By searching for specific error messages, directory listings, or vulnerable software versions, they can uncover weaknesses that can be exploited. This helps in assessing the security posture of the target and prioritizing remediation efforts.  
  
-Exploitation Validation: After identifying potential vulnerabilities, ethical hackers can use Google hacking to verify if those vulnerabilities are exploitable. By searching for known exploits, proof-of-concept code, or vulnerability disclosures, they can validate the feasibility and impact of an identified vulnerability. This helps in demonstrating the real-world impact of a vulnerability and aids in effective risk assessment and mitigation.

**Name five methods for obtaining more specific search results. For more information, read the following article.**  
1) Exact phrase(" ")  
2) Exclude words(-)  
3)Unknown terms(\*)  
4)File type  
5)Inurl

**Think of an example of each of the search methods you mentioned in the previous question. You can add these examples in the relevant place in the previous question.**  
1) "Cybersecurity"  
2) Cyber -security  
3)\*Cybersecurity  
4) Cybersecurity filetype:pdf  
5)inurl: Cybersecurity

**How would you search for each of the following demands?&nbsp;  
  
  
Pictures of only teacup pigs  
A PDF document about hand sanitizers  
A picture of a mouse, but not a computer mouse**  
“teacup pigs” | +teacup +pig

filetype:pdf “hand sanitizers”

“mouse -computer”

# Question 8

**In which situations would you use Google hacking techniques?**  
- To anonymously gather information about targets.  
- To find leaked credentials and other sensitive data.  
- To find personal information, such as email addresses and contact details.  
- To create a footprint fornetwork-connected devices and services.

# Question 9

**Nmap is a port scanner tool used for network discovery.&nbsp;  
  
Name at least five features that Nmap provides its users.**  
Host discovery  
Port discovery / enumeration  
Service discovery  
Operating system version detection  
Hardware (MAC) address detection  
Service version detection  
Vulnerability / exploit detection, using Nmap scripts (NSE)  
Nmap IDS / Portscan Detection & Scan Time Optimisation

**Let’s look at the target IP address 192.168.1.10. For each of the following questions, write the relevant command.&nbsp;  
  
  
Scan the address  
Scan the address and the next 20 addresses  
Scan the machines in the subnet 192.168.1.0/8 that respond to a ping  
Scan ports 10-1010  
Scan the address and fetch the service versions  
Scan the address to detect a firewall or packet filters  
Scan the address, as well as the address 192.168.1.15**  
-nmap 192.168.1.10  
-nmap 192.168.1.10-30  
-nmap -sP 192.168.1.0/8  
-nmap -p 10-1010 192.168.1.10  
-nmap -sV 192.168.1.10  
-nmap -sA 192.168.1.10  
-nmap 192.168.1.10 192.168.1.15

**Explain the Aggressive Detection command.**  
The Aggressive Detection command in Nmap is a parameter that enables a comprehensive and aggressive scan against the target system. It is designed to provide an extensive range of tests and probes to gather as much information as possible about the target's services, operating system, and potential vulnerabilities.  
  
The Aggressive Detection command is executed using the -A option in Nmap. Here's an example of how to use it:  
nmap -A <target>  
Enable OS detection, version detection, script scanning, and traceroute.

**There are several types of Nmap scans. Name three types and explain them.&nbsp;  
  
For additional help, check out the following webpage.**  
TCP SCAN  
A TCP scan is generally used to check and complete a three-way handshake between you and a chosen target system. A TCP scan is generally very noisy and can be detected with almost little to no effort. This is “noisy” because the services can log the sender IP address and might trigger Intrusion Detection Systems.  
  
UDP SCAN  
UDP scans are used to check whether there is any UDP port up and listening for incoming requests on the target machine. Unlike TCP, UDP has no mechanism to respond with a positive acknowledgment, so there is always a chance for a false positive in the scan results. However, UDP scans are used to reveal Trojan horses that might be running on UDP ports or even reveal hidden RPC services. This type of scan tends to be quite slow because machines, in general, tend to slow down their responses to this kind of traffic as a precautionary measure.  
  
SYN SCAN  
This is another form of TCP scan. The difference is unlike a normal TCP scan, nmap itself crafts a syn packet, which is the first packet that is sent to establish a TCP connection. What is important to note here is that the connection is never formed, rather the responses to these specially crafted packets are analyzed by Nmap to produce scan results.  
  
ACK SCAN  
ACK scans are used to determine whether a particular port is filtered or not. This proves to be extremely helpful when trying to probe for firewalls and their existing set of rules. Simple packet filtering will allow established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not.

**Explain at least one advantage and one disadvantage of every scan type you mentioned in the previous question.**  
TCP scan  
Advantage:  
Accurate Port Detection: TCP scanning provides accurate results regarding the open ports on a target system. By sending TCP packets to different port numbers and analyzing the responses, TCP scanning can determine which ports are open, closed, or filtered. This information is valuable for understanding the network's services and potential entry points for further assessment or exploitation.  
Disadvantage:  
Noisy and Easily Detectable: TCP scanning involves sending packets to a range of ports, which can generate network traffic and raise alarms in intrusion detection systems (IDS) or firewall logs. This makes it more likely to be detected by network administrators or security systems, potentially alerting them to the scanning activity. Additionally, some network devices and firewalls may be configured to block or rate-limit scanning attempts, limiting the effectiveness of TCP scanning.  
UDP scan  
Advantage:  
Broad Service Coverage: UDP scanning allows for the detection of services that use the UDP protocol, which is commonly used for services like DNS, DHCP, SNMP, and more. By sending UDP packets to specific port numbers and analyzing the responses, UDP scanning can identify open UDP ports, providing a more comprehensive understanding of the network services available.  
Disadvantage:  
Unreliable and Unresponsive Targets: UDP scanning relies on the response of the target system's UDP services. However, UDP is connectionless and does not provide guaranteed delivery or response. This makes UDP scanning less reliable than TCP scanning, as many UDP services may not respond to scanning probes, resulting in potentially false negatives or inconclusive results. Additionally, firewalls and network devices may block or filter UDP traffic, making it challenging to accurately determine the status of UDP ports.  
SYN scan  
Advantage:  
Stealthy and Fast: SYN scanning is considered a stealthy scanning technique because it does not establish a full TCP connection with the target system. Instead, it sends SYN packets and analyzes the response behavior. This approach makes SYN scanning harder to detect by intrusion detection systems (IDS) and firewall logs. Additionally, SYN scanning is generally faster compared to other scanning techniques, as it only initiates a partial handshake with the target system.  
Disadvantage:  
Incomplete Response Analysis: SYN scanning relies on the behavior of the target system's response to SYN packets. However, not all systems respond consistently or predictably to SYN packets. Some systems may respond with SYN/ACK, RST, or no response at all. This can lead to incomplete or ambiguous results, making it more challenging to accurately determine the status of ports. As a result, further scanning or analysis may be required to confirm open or closed ports.  
ACK scan  
Advantage:  
Firewall Rule Analysis: ACK scanning is primarily used to analyze how a target system's firewall or packet filtering rules are configured. By sending ACK packets with specific flag combinations, ACK scanning examines the response behavior of the target system. It helps identify whether packets are allowed, filtered, or blocked by the firewall. This information is valuable for understanding the network's security measures and potential weaknesses in the filtering rules.  
Disadvantage:  
Limited Port Detection: Unlike other scanning techniques, ACK scanning does not provide comprehensive port detection or service identification. It focuses specifically on evaluating firewall filtering rules and does not directly identify open or closed ports on the target system. ACK scanning alone cannot determine the state of ports or services, making it necessary to combine it with other scanning techniques for a more complete assessment.

# Question 10

**As a future cyber security expert, in which situations would you use Nmap? Give an example.**  
As a future cybersecurity expert, you would use Nmap in various situations to conduct network scanning and security assessments. Here are a few examples:  
  
**Vulnerability Assessment**: Nmap can be used to perform a vulnerability assessment on a target network. By scanning for open ports, identifying services, and detecting software versions, you can cross-reference this information with vulnerability databases to identify potential security weaknesses and prioritize remediation efforts.  
  
**Penetration Testing:** During a penetration testing engagement, Nmap is a valuable tool for mapping the target network, identifying potential entry points, and understanding the network's security posture. It helps in locating exposed services, determining if they are properly secured, and finding potential vulnerabilities that can be exploited.  
  
**Network Inventory:** Nmap can be utilized to create an inventory of devices and systems within a network. By performing host discovery and port scanning, you can identify active hosts, determine their IP addresses, and gather information about the network devices and services running on them. This assists in maintaining an up-to-date inventory and understanding the network's composition.  
  
**Incident Response:** In the event of a security incident, Nmap can be employed to quickly assess the impact and scope of the incident. By scanning affected systems, identifying open ports, and analyzing network traffic, you can gather crucial information to aid in the investigation, containment, and recovery processes.  
  
**Network Hardening:** Nmap can be used proactively to assess the security of your own network and identify potential vulnerabilities or misconfigurations. By scanning your network periodically, you can ensure that only necessary ports are open, services are properly configured, and security measures are in place to defend against potential threats.