PenTest+ Quizzes

## **Domain 1**

1. If you have a smaller budget allocated for your penetration test, which of the following would most likely occur?

1. Increased timeline for testing
2. Increase scope
3. Increase resources
4. **Increase constraints**

Explanation: If you are provided with a smaller budget, generally your penetration test will be more limited in scope, time allocated, resources allocated, and have additional constraints placed upon it.

2. Which of the following is part of Rules of Engagement?

1. Timeline
2. Location
3. Test boundaries
4. **All of the above**

Explanation: Rules of Engagement include the timeline, location, test boundaries, and other rules that must be followed during the penetration test.

3. Which of the following will determine how long the test will be conducted?

1. **Timeline**
2. Location
3. Test boundaries
4. All of the above

Explanation: The timeline will establish how long the penetration testing activities can be conducted for and when they can be started.

4. Which of the following will determine the certain time that testing is not authorized?

1. Timeline
2. Transparency
3. **Time restriction**
4. Budget

Explanation: Time restrictions may be agreed upon and placed in the Rules of Engagement in order for the pentesting team to only operate during certain times of day or to avoid certain days altogether.

5. Which of the following will determine what will be tested?

1. Timeline
2. **Test Boundaries**
3. Location
4. Time restriction

Explanation: Test boundaries are used to create the scope of what will and will not be tested during the penetration test.

6. Which type of hackers always get permission before doing a penetration testing?

1. **White hat hacker**
2. Gray hat hacker
3. Black hat hacker
4. Red hat hacker

Explanation: White hat hackers, also known as ethical hackers or penetration testers, will always get permission from the appropriate authority within a company prior to beginning a penetration test on the organization’s network.

7. If the organization is hosting their servers and services in a cloud based solution, whose permission do you need prior to beginning the penetration test?.

1. Organization
2. Cloud provider
3. **Both the organization and the cloud provider**
4. Neither the organization nor the cloud provider

Explanation: You must gain the permission from both the organization and the cloud provider prior to beginning your penetration test.

8. What formal document is created to document what work will and will not be performed during a penetration test?

1. Master Service Agreement (MSA)
2. Non-Disclosure Agreement (NDA)
3. **Statement of Work (SOW)**
4. Payment agreement

Explanation: A Statement of Work (SOW) is a document routinely employed to define project-specific activities, deliverables, and timelines that a penetration testing company will provide to their client during an assessment.

9. Which type of box simulates an outside attack?

1. White box
2. **Black box**
3. Grey box
4. None of the above

Explanation: Black-box testing is a method of penetration testing that examines the network and systems without any prior knowledge as to its internal design or structure.

10. What group has the best capability and intent to hack a particular network or system and conducts highly covert hacks over long periods of time?

1. **Advanced Persistent Threat (APT)**
2. Hacktivist
3. Insider Threat
4. Script Kiddies

Explanation: An advanced persistent threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time. APTs are highly organized and well-funded.

## **Domain 2**

1. \_\_\_\_\_\_ Is a systematic attempt to locate, gather, identify, and record information about a target.

1. **Reconnaissance**
2. Enumeration
3. Certificate Inspection
4. Packet Capture

Explanation: Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible.

2. Which of the following is NOT a tool used during the reconnaissance phase?

1. Ping
2. Google
3. **John the Ripper**
4. Maltego

Explanation: John the Ripper is used to conduct password cracking, therefore it is better categorized as an exploitation tool. The other tools are all used in the reconnaissance phase.

3. What term best describes actively connecting to a target in order to get a response which identifies the open ports and services on a system?

1. Fingerprinting
2. **Scanning**
3. Cryptographic Inspection
4. None of the above

Explanation: Scanning is used to identify live hosts, ports, and services, to discover the operating system and architecture of target system, and to identify the vulnerabilities and threats in the network.

4. What process is used to manually enumerate a system by analyzing the captured packets to determine information?

1. **Packet inspection**
2. Cryptographic inspection
3. Packet crafting
4. Certificate inspection

Explanation: Packet inspection is conducted by analyzing the captured network packets in order to manually enumerate a system and gain additional information.

5. What process is used to determine the encryption being used by a system?

1. Packet inspection
2. **Cyptographic inspection**
3. Packet crafting
4. Certificate inspection

Explanation: Cryptographic inspection occurs during the information gathering stage to determine the level and type of encryption being used by a system.

6. What process is used to intercept and log network traffic that can be seen via the wired or wireless network interface?

1. Cyptographic inspection
2. **Network traffic sniffing**
3. Packet Capture
4. Decompiling

Explanation: Network traffic sniffing is used to intercept and log network traffic that can be seen via the wired or wireless network interface device.

7. What is the term for the process of reverse engineering software using a decompiler?

1. Cyptographic inspection
2. Sniffing network traffic
3. Packet Capture
4. **Decompiling**

Explanation: Decompiling is the process of reverse engineering software using a decompiler.

8. What is the process of identifying and removing errors from hardware, software, or systems called?

1. Decompiling
2. **Debugging**
3. Scrapping
4. Programming

Explanation: Debugging is the process of identifying and removing errors from hardware, software, or systems.

9. Which of the following is true for credentialed scans?

1. The scanner does not have a user or admin account.
2. It is considered closer to the hacker’s perspective.
3. **The scanner uses an authorized user or admin account.**
4. It must be initiated from within the network.

Explanation: Credentialed scans require an authorized username and password to be provided to the scanning engine, but they do not have to be initiated from within the network. This type of scan provides you with the view an insider might hack, not an external hacker or attacker.

10. Which of the type of scans is the least intrusive scan?

1. **Discovery scan**
2. Full scan
3. Stealth scan
4. Compliance scan

Explanation: A discovery scan in Nmap is used to perform a quick scan using pings to identify what devices or systems are on the network. It is the least intrusive and intensive scan of the options provided.

## **Domain 3**

1. What is a kind of attack that lures people into providing sensitive data mostly by using email?

1. **Phishing**
2. Interrogation
3. Impersonation
4. Shoulder Surfing

Explanation: Phishing is a social engineering attack that attempts to trick a user into provided sensitive details by deceiving them with a well-crafted email.

2. What is is called when a phishing attempt that occurs over a text message?

1. **SMS Phishing**
2. Impersonation
3. Interrogation
4. Vishing

Explanation: SMS Phishing is an evolution of phishing which uses SMS and text messages to trick a user into providing personal information to the attacker.

3. What is the act of pretending to be someone else in order to gain access or gather information called?

1. Phishing
2. **Impersonation**
3. Interrogation
4. Shoulder Surfing

Explanation: Impersonation is the act of pretending to be someone else in order to gain access or gather information. A common impersonation technique is to dress up as a delivery driver to gain access to a facility.

4. Which of the following is a motivation factor that might be used to get an employee to comply with your request for assistance or information?

1. Authority
2. Urgency
3. Social Proof
4. **All of the above**

Explanation: Authority, urgency, and social proof are all valid techniques to get an employee to comply with your requests for assistance or information.

5. What is it called when a pentester follows an authorized individual into a secure location?

1. **Tailgating**
2. Dumpster Diving
3. Lock Picking
4. Lock Bypass

Explanation: Tailgating occurs when a pentester follows an authorized individual into a secure location.

6. What is it called when a pentester looks through the trash or recycling of an organization?

1. Tailgating
2. **Dumpster Diving**
3. Lock Picking
4. Egress Sensor

Explanation: Dumpster diving is a reconnaissance technqiue used by pentesters that involves searching through an organization’s trash or recycling bins to find useful information.

7. What protocol is considered the Internet standard for electronic mail transmissions?

1. FTP
2. SNMP
3. **SMTP**
4. DNS

Explanation: The Simple Mail Transfer Protocol (SMTP) is the Internet standard for sending email and operates on port 25.

8. What attack allows DNS poisoning that occurs on the local computer or server?

1. **DNS Cache Poisoning**
2. Pass The Hash
3. Hash Poisoning
4. DNS Poisoning

Explanation: DNS Cache Poisoning occurs on the local computer or server instead of the DNS server itself.

9. What attack occurs when a website’s encryption is tricked into presenting the user with a HTTP connection instead of a HTTPS connection?

1. DNS poisoning
2. **Downgrade**
3. Relay
4. ARP Spoofing

Explanation: SSL Stripping is a specific type of downgrade attack that can be performed to force a user’s browser into making an unsecure HTTP connection instead of a secure HTTPS connection.

10. What type of attack is conducted by exhausting all available resources?

1. Relay
2. Downgrade
3. **Denial of Service**
4. VLAN Hopping

Explanation: A Denial of Service (DOS) attack is conducted by exhausting all the available resources available on a service or server to prevent authorized users from gaining access or use of the resources.

## **Domain 4**

1. Which of the following is a function of Nmap?

1. Command line tool that sends specially crafted packets to the target host(s) of a network
2. Discovers the hosts and services being run based on the responses received
3. **Both A and B**
4. None of the above

Explanation: Nmap is a command line tool that sends specially crafted packets to the target host(s) of a network and can be used to discover hosts and services being run based on the responses it receives during a scan.

2. What Nmap command is used for version detection of the services and applications being run on a given port?

1. Nmap -sS
2. Nmap -sT
3. **Nmap -sV**
4. Nmap -p

Explanation: Nmap -sV scans the targets open ports and attempts to identify the services/applications running on those ports and their associated versions.

3. Which of the following Nmap command is for setting the timing for the scan?

1. Nmap -Pn
2. Nmap -iL
3. **Nmap -T**
4. Nmap -p

Explanation: Nmap -T is used to set the timing of the scans that will occur, with -T5 being fastest and -T0 being slowest.

4. What is the process of collecting information before attacking a system or server called?

1. **Reconnaissance**
2. Exploitation
3. Vulnerability Scanning
4. Credential Attacks

Explanation: Reconnaissance is the process of collecting information about a system prior to attempting to connect to it.

5. What is the term for the activities that involve ensuring a system meets a given security baseline or policy?

1. Reconnaissance
2. Credential Attacks
3. Vulnerability Scanning
4. **Configuration Compliance**

Explanation: Configuration compliance is the activities involved in ensuring a system meets a given security baseline or policy.

6. What is the tool IDA used for?

1. Evasion
2. **Decompilation**
3. Software Assurance
4. None of the above

Explanation: IDA is a commonly used and quite popular decompiler.

7. Which of the following is not commonly used for debugging software?

1. **Nmap**
2. GDB
3. IDA Pro
4. Ollydbg

GDB, IDA Pro, and Ollydbg are all commonly used debugging tools. Nmap is not considered a debugging tool, but could be helpful during network troubleshooting.

8. Which of the following is not considered a password cracker?

1. John the ripper
2. Hydra
3. Cain and Abel
4. **OpenVAS**

Explanation: OpenVAS is a vulnerability scanner. The other three tools are password crackers.

9. Which of the following tool could be used to analyze malware and reverse engineer binary files?

1. Dirbuster
2. Patator
3. Mimikatz
4. **Immunity Debugger**

Explanation: Immunity debugger is useful in malware analysis and reverse engineering of binary files.

10. What tool is used in wireless hacking and contains a scanner, packet sniffer, and password cracker?

1. Censys
2. Maltego
3. **Aircrack-NG**
4. Shodan

Explanation: Aircrack-NG is the most popular wireless hacking suite in use. It providers a wireless scanner, packet sniffer, and password cracker as part of its features.

## **Domain 5**

1. What is the process of combining data from multiple sources and formats into a common and consistent event format called?

1. **Normalization**
2. Communication Paths
3. Goal Reprioritization
4. Situation Awareness

Explanation: Normalization is the process of combining data from multiple sources and formats into a common and consistent event format.

2. What is the process of determining if the detected activity was performed by a hacker or a authorized penetration tester?

1. Situation Awareness
2. **Deconfliction**
3. De-escalation
4. Triggers

Explanation: Deconfliction is the process of determining if the detected activity was performed by a hacker or a authorized penetration tester.

3. True or False: Findings and recommendations are sensitive in nature and should be treated as confidential.

1. **True**
2. False

Explanation: True. It is important to keep the findings from your penetration test confidential from personnel without the need to know since it contains all the details of how to break into a company’s network.

4. True or False: Your final report should only contain a list of vulnerabilities you found.

1. True
2. **False**

Explanation: False. Your final report should include not only a list of vulnerabilities you found, but also a prioritized list of recommendations on how to secure the network.

5. Which of the following is not consider one of the five authentication factors?

1. Something you know
2. Something you have
3. Something you are
4. **Something you want**

Explanation: The five authentication factors are something you know (knowledge), something you have (possession), something you are (biometrics), somewhere you are (location), and something you do (action).

6. Which of the following is not part of Post-Report activities?

1. Post-engagement cleanup
2. Attestation of findings
3. Client acceptance
4. **Footprinting**

Explanation: Footprinting occurs during the reconnaissance and information gathering phase. Post-engagement cleanup, attestation of findings, and client acceptance all considered post-report activities.

7. What document is signed at the end of a penetration testing engagement by the client to signify completion of all required work product under your contract?

1. Non-Disclosure Agreement (NDA)
2. Statement of Work (SOW)
3. **Client Acceptance**
4. Payment agreement

Explanation: Client acceptance is a formal document that is signed at the conclusion of the penetration testing engagement. It signifies that the client agrees you have fulfilled everything listed in the scope of work.

8. Which of the statement is not true concerning the data you collect during a penetration test?

1. All of the passwords must be stored as hashes or in another encrypted format.
2. All of the assessment data should always be handled with due diligence and care.
3. All the data must be aggregated, normalized, and correlated in order for it to become understandable and useful.
4. **All three statements are considered true**

Explanation: All three statements are considered true regard the data you collect during a penetration test.

9. What is an artifact that you might observe on a network or system during your penetration test that would cause you to state that the network has been exploited previously?

1. States
2. Critical findings
3. **Indicator of compromise**
4. Communication paths

Explanation: An indicator of compromise is an artifact that you might observe on a network or system during your penetration test that would cause you to state that the network has been exploited previously.

10. What statement regarding communication is true?

1. **Communication is required before, during, and after a penetration test.**
2. Communication is required before and after a penetration test, but not during one.
3. Communication is required before a penetration test, but not during or after one.
4. Communication is required during and after a penetration test, but not before one.

Explanation: It is a best practice to communicate with the targeted organization before, during, and after the penetration test. It is important to ensure you have a good trusted agent within the organization during the penetration test so that the pentester’s attacks can be deconflicted from real world events.