Pentest+

Study online at https://quizlet.com/_fhyeuv

Which of the following types of agreements is used to document the commitment between a provider and client in terms of quality and availability?	SLA
You are working as part of a penetration testing team conducting engagement against Dion Training's network. You have been given a list of targets in a text file called servers.txt. Which of the following Nmap commands should you use to find all the servers from the list with ports 80 and 443 enabled and save the results in a greppable file called results.txt?	nmap -p80,443 -iL servers.txt -oG results.txt
Which of the following is the most difficult to confirm with an external vulnerability scan?	Blind SQL injection
Which of the following tools should a penetration tester use to debug a Windows executable in Kali Linux?	Ollydbg
What nmap switch would you use to determine which UDP ports are open on a targeted network?	-sU
Which of the following penetration testing methodologies or frameworks is an open-source collection of documents that outlines every area of an organization that needs to undergo testing, as well as provides details on how those tests should be conducted?	Open source security testing methodology manual (OSSTMM)
Which of the following penetration testing methodologies is focused on testing web applications and the people, processes, and technology that support them?	OWASP Testing guide (OTG)
Which of the following tools should a penetration tester use when debugging a binary on the Windows operating system?	WinDbg
Which of the following tools should a penetration tester use to brute-force authentication on ftp, ssh, smb, vnc, or zip archive passwords?	Patator
Wget, nc, telnet	Banner grabbing
After issuing the command "telnet diontraining.com 80" and connecting to the server, what command conducts the banner grab?	HEAD / HTTP/1.1
Which of the following tools is considered a web application scanner?	ZAP
You are preparing for an upcoming penetration test. You want to begin your reconnaissance but need to validate the scope of the IP addresses and the times of day you can scan the network. Which of the following documents should you refer to find these details?	ROE (Rules of engagement)
You want to conduct OSINT against an organization in preparation for an upcoming engagement. Which of the following tools should you utilize?	Shodan
Which of the following penetration testing methodologies or frameworks was developed by business professionals as a best practice guide for conducting penetration tests?	Penetration Testing Execution Standard (PTES)
Dion Training has hired you to assess its voucher fulfillment REST API on its e-commerce website. Which of the following support resources would be MOST helpful when conducting a known-environment assessment of the API?	Swagger document
Which of the following tools should a penetration tester use to automatically gather details about plugins used on a WordPress site and compare them against a database of known vulnerabilities?	WPScan
Which of the following tools is used by a penetration tester to conduct open-source intelligence (OSINT)?	Maltego
You have been contracted to conduct a compliance-based assessment for an organization. What is the MOST important thing for you to understand?	The organization's industry

You are working as part of a penetration testing team targeting Dion Training's website. Which of the following tools should you use to attempt an XSS or injection attack against their website?	BeEF
Which of the following tools allows a penetration tester to quickly locate exploits in the Exploit Database archive?	SearchSploit
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You are reviewing the DNS records for the company and are trying to identify which third-party hosted services they may be using. Which of the following DNS records should you analyze to identify any human-readable records, domain verifications, and domain authentications	TXT
Which of the following types of information is protected by rules in the United States that specify the minimum frequency of vulnerability scanning required for devices that process it?	Credit card data
What is a common technique used by malicious individuals to perform an on-path attack on a wireless network?	An evil twin
Dion Training has hired you to assess its voucher fulfillment web application on its e-commerce website. The web application relies on a SOAP-based web service. Which of the following support resources would be MOST helpful in conducting this known-environment assessment?	WSDL Document
What tool is used to collect wireless packet data?	Aircrack-ng
You are performing a web application security test, notice that the site is dynamic, and must be using a back-end database. You decide you want to determine if the site is susceptible to an SQL injection. What is the first character that you should attempt to use in breaking a valid SQL request?	Single quote
Which of the following tools should a penetration tester use to conduct a vulnerability scan of a web application to identify if it is subject to an injection exploit?	Wapiti
Which of the following is a special type of embedded operating system that uses a predictable and consistent scheduler?	RTOS
Which of the following tools should a penetration tester use to create a word list based on text and metadata from a target organization's website?	CEWL
Which file on a Linux system is modified to set the maximum number of days before a password must be changed?	/etc/shadow
Which of the following tools should a penetration tester use to conduct password cracking of multiple network authentication types simultaneously?	Hydra
Which of the following tools is a post-exploitation framework that would allow a penetration tester to run PowerShell agents without requiring the use of powershell.exe?	Empire
Which of the following tools provides a penetration tester with Python classes with low-level program access to packets, protocols, and their implementation?	Impacket
Which of the following tools should a penetration tester use to identify and exploit web-based vulnerabilities, such as SQL injections and cross-site scripting attacks?	w3af
Which of the following tools should a penetration tester use as a .NET framework to conduct penetration testing and debugging?	Covenant
Which of the following tools should a penetration tester use to gather credentials by extracting cleartext passwords, hashes, and PIN codes from a victimized machine's memory?	Mimikatz

Your company is expanding its operations in the European Union and is concerned about additional governmental regulations that may apply. Which of the following regulations applies when processing personal data within the European Union?	GDPR
A user receives certificate errors in other languages within their web browser when accessing your company's website. Which of the following is the MOST likely cause of this issue?	On-path attack
Which of the following rules of engagement provides the days and times that the penetration test can occur?	Temporal restrictions
Which of the following might be exploited on a Linux server to conduct a privilege escalation?	Insecure sudo
Which of the following lateral movement techniques provides an HTTP Simple Access Object Protocol (SOAP) standard for specific remote management services on Windows systems?	WinRM
You are working as part of a penetration testing team targeting Dion Training's Linux-based network. You want to determine if you can crack the password on their remote authentication servers. Which of the following tools should you use?	Medusa
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify any web pages that contain the term "password" and whose URL contains diontraining.com in the hyperlink displayed on the page. Which of the following Google hacking queries should you use?	passwordinanchor:diontraining.com
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify any domain names also covered by the organization's digital certificate to include in your assessment. Which of the following should you review to determine any other domains that can use the same digital certificate?	SAN
Which of the following tools should a penetration tester use to enumerate user accounts, escalate privileges, and other tasks during the post-exploitation phase against an AWS-based cloud architecture?	Pacu
You are conducting a vulnerability assessment when you discover a critical web application vulnerability on one of your Apache servers. Which of the following files would contain the Apache server's logs if your organization uses the default naming convention?	access_log
Which of the following tools should a penetration tester use to identify hidden directories, files, or subdomains by brute force?	Gobuster
A penetration tester wants to install an integrated platform for testing web applications. The software should allow them to capture, analyze, and manipulate HTTP traffic. Which of the following tools should they install?	Burp suite
Which of the following open source tools should a penetration tester use to conduct vulnerability scans against a company's infrastructure?	OpenVAS
Which of the following tools should a penetration tester use to conduct packet manipulation by crafting and sending malformed packets to a network target?	Scapy
Which of the following tools provides a penetration tester with the ability to mask their identity and source IP address by sending messages through intermediaries?	ProxyChains
You have been given access to a Windows system located on an Active Directory domain as part of a known environment	net view

penetration test. Which of the following commands would provide information about other systems on this network?	
Which of the following methodologies or frameworks provides a matrix that describes the different tasks conducted by an attacker or penetration tester during an engagement?	MITRE ATT&CK framework
What is a legal contract that outlines the guidelines for any business documents and contracts between two parties?	MSA
What is a common Service Oriented Architecture Protocol (SOAP) vulnerability?	XML Denial of service
You are working as part of a penetration testing team targeting Dion Training's webserver. You want to determine if you can expose any directories or file names on the webserver. Which of the following tools should you use?	Dirbuster
Which of the following tools provides a penetration tester with a framework to conduct technical social engineering attacks like phishing against an organization's employees?	SET
If an attacker can compromise an Active Directory domain by utilizing an attack to grant administrative access to the domain controllers for all domain members, which type of attack is being used?	Golden ticket attack
Which of the following penetration testing methodologies or frameworks provides an open-source resource that includes documents relating to penetration testing, guidelines on business continuity and disaster recovery, as well as legal and regulatory compliance guidelines?	ISSAF
Which of the following tools should a penetration tester use to conduct post-exploitation identification of vulnerabilities in a Windows Active Directory environment?	CrackMapExec
You are conducting a quick nmap scan of a target network. You want to conduct an SYN scan, but you don't have raw socket privileges on your workstation. Which of the following commands should you use to conduct the SYN scan from your workstation?	Nmap -sT