Pen5

Study online at https://quizlet.com/_fi2w3t

You have been contracted to conduct a wireless penetration test for a corporate client. Which of the following should be documented and agreed upon in the scoping documents before you begin your assessment? A) The make and model of the wireless access points used by the client B) The number of wireless access points and devices used by the client C) The frequencies of the wireless access points and devices used by the client D) The network diagrams with the SSIDs of the wireless access points used by the client	C. To ensure you are not accidentally targeting another organization's wireless infrastructure during your penetration test, you should have the frequencies of the wireless access points and devices used by the client documented in the scoping documents. This would include whether your clients use Wireless A, B, G, N, or AC and if they are using the 2.4 GHz or 5.0 GHz spectrum if they are using Wireless N or AC.
A vulnerability scan has returned the following results: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Detailed Results 10.56.17.21 (APACHE-2.4) Windows Shares Category: Windows CVE ID: - Vendor Ref: - Bugtraq ID: - Service Modified - 8.30.2017 Enumeration Results: print$ c:\windows\system32\spool\drivers files c:\FileShare\Accounting Temp c:\temp -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- What best describes the meaning of this output? A) There is an unknown bug in an Apache server with no Bugtraq ID B) Connecting to the host using a null session allows enumeration of the share names on the host C) Windows Defender has a known exploit that must be resolved or patched D) There is no CVE present, so this is a false positive caused by Apache running on a Windows server	B. These results from the vulnerability scan conducted shows an enumeration of open Windows shares on an Apache server. The enumeration results show three share names (print$, files, Temp) were found using a null session connection. There is no associated CVE with this vulnerability, but it is not a false positive. Not all vulnerabilities have a CVE associated with them. Nothing in this output indicates anything concerning Windows Defender, so this is not the correct answer. Bugtraq IDs are a different type of identification number issued for vulnerabilities by SecurityFocus. Generally, if there is a CVE, there will also be a Bugtraq ID. Both the CVE and Bugtraq ID being blank is not suspicious since we are dealing with a null enumeration result.
You were interpreting a Nessus vulnerability scan report and identified a vulnerability in the system with a CVSS attack vector rating of A. Based on this information, which of the following statements would be true? A) The attacker must have physical or logical access to the affected system B) Exploiting the vulnerability requires the existence of specialized conditions C) The attacker must have access to the local network that the system is connected to D) Exploiting the vulnerability does not require any specialized conditions	C. The attack vector explains what type of access that the attacker must have to a system or network and does not refer to the types of specialized conditions that must exist. In this case, the A rating refers to Adjacent, where the attacker must launch the attack from the same shared physical (such as Bluetooth or Wi-Fi network), logical network (such as a local subnet), or a limited administrative domain (such as a VPN or MPLS). An attack vector of Network (N) would allow the attack to extend beyond these options and conduct remote exploitation of the vulnerability. An attack vector of Local (L) would require the attacker to locally exploit the workstation via the keyboard or over an SSH connection. An attack vector of Physical (P) would require the attacker to physically touch or manipulate the vulnerable component themselves, such as conducting a cold boot attack.
What type of technique does exploit chaining often implement? A) Injecting parameters into a connection string using semicolons as a separator B) Inserting malicious JavaScript code into input parameters C) Setting a user's session identifier (SID) to an explicit known value D) Adding multiple parameters with the same name in HTTP requests	A. Connection String Parameter Pollution (CSPP) exploits specifically the semicolon-delimited database connection strings that are constructed dynamically based on the user inputs from web applications. CSPP, if carried out successfully, can be used to steal user identities and hijack web credentials. CSPP is a high-risk attack because of the relative ease with which it can be carried out (low access complexity) and the potential results it can have (high impact). Exploit chaining involves multiple commands and exploits being conducted in a series to fully attack or exploit a given target.

Your network security manager wants a monthly report of the security posture of all the assets on the network (e.g., workstations, servers, routers, switches, firewalls). The report should include any feature of a system or appliance that is missing a security patch, OS update, or other essential security feature and its risk severity. Which solution would work best to find this data? A) Security policy B) Penetration test C) Virus scan D) Vulnerability scanner	D. A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses. Most vulnerability scanners also create an itemized report of their findings after the scan.
You have received a laptop from a user who recently left the company. You went to the terminal in the operating system and typed 'history' into the prompt and see the following: -=-=-=-=-=-=-=-=-=-=-=-=-=- > for i in seq 255; ping -c 1 10.1.0.$i; done -=-=-=-=-=-=-=-=-=-=-=-=-=- Which of the following best describes what actions were performed by this line of code? A) Attempted to conduct a SYN scan on the network B) Conducted a ping sweep of the subnet C) Conducted a sequential ICMP echo reply to the subnet D) Sequentially sent 255 ping packets to every host on the subnet	B. This code is performing a ping sweep of the subnet 10.1.0.0/24. The code states that for every number in the sequence from 1 to 255, conduct a ping to 10.1.0.x, where x is the number from 1 to 255. When it completes this sequence, it is to return to the terminal prompt (done). The ping command uses an echo request and then receives an echo reply from the ping's target. A ping sweep does not use an SYN scan, which would require the use of a tool like nmap or hping.
Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host? A) netcat B) telnet C) wget D) ftp	D. FTP cannot be used to conduct a banner grab. A cybersecurity analyst or penetration tester uses a banner grab to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. This is commonly done using telnet, wget, or netcat.
Due to new regulations, your organization's CIO has the information security team institute a vulnerability management program. What framework would BEST support this program's establishment? A) NIST B) OWASP C) SDLC D) SANS	A. NIST (National Institute of Standards and Technology) produced a useful patch and vulnerability management program framework in its Special Publication (NIST SP 800-40). It would be useful during the program's establishment and provide a series of guidelines and best practices. SANS is a company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC). The SDLC is the software development lifecycle. It is a method for dividing programming projects into separate phases. The Open Web Application Security Project (OWASP) is a community effort that provides free access to many secure programming resources. The resources provided include documentation on web app vulnerabilities and mitigation tactics, software tools used to identify and handle threats that target web applications, frameworks for secure development life cycle implementation, frameworks for penetration testing web apps, general secure coding best practices, guidelines for specific web-based languages, and more.
What command could be used to list the active services from the Windows command prompt? A) sc query type= running B) sc query \\servername C) sc query D) sc config	C. Windows uses the sc query to display information about the running service. It is part of the Service Control command-line tool, known as sc. The sc config command will modify the value of a service's entries in the registry and the Service Control Manager database. The sc query command will obtain and display information about the specified service, driver, type of service, or driver type. By entering just the sc query, the command will return the information on the active services only. By using the type=running option, only the information on the running service will be displayed. If the command sc query \\servername is used, then the remote server's active services (\\servername) will be displayed.

You have just conducted an automated vulnerability scan against a static webpage without any user input fields. You have been asked to adjudicate the scanner's findings in the automated report. Which of the following is MOST likely to be a false positive? A) Reflected XSS B) Insecure HTTP methods allowed C) Command injection allowed D) Directory listing enabled	C. A command injection is unlikely since this is a static webpage and does not accept any user input. A command injection allows the user to supply malicious input to the web server and then passes that data to a system shell for execution. In this sense, command injection does create new instances of execution and can, therefore, leverage languages that the web app does not directly support.
A security analyst wants to implement a layered defense posture for this network, so he uses multiple antivirus defensive layers, including both an end-user desktop antivirus software and an email gateway scanner. What kind of attack would this approach help to mitigate? A) Forensic attack B) ARP spoofing attack C) Social engineering attack D) Scanning attack	C. By utilizing both endpoint protection (desktop antivirus software) and the email gateway scanner, the security analyst works to prevent phishing and other social engineering attacks. Emails are a common attack vector used in social engineering attacks.
Which of the following might be exploited on a Windows server to conduct a privilege escalation? A) Ret2libc B) Sticky bits C) SAM database D) SUID/SGID programs	C. The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista, Windows 7, 8.1, and 10 that stores users' passwords. It authenticates local and remote users. The SAM uses cryptographic measures to prevent unauthenticated users from accessing the system but could be cracked offline using a password cracker to determine the administrative user's passwords. Ret2libc, sticky bits, and SUID/SGID programs are WindLinuxows-specific privilege escalation techniques.
BigCorpData recently had suffered a massive data breach caused by a hacker. You have been hired as an expert to assist in their incident response and recovery. You look through the shell history on a Linux server and see the following entry: # echo " " > /var/log/syslog. Which of the following techniques did the attacker use to attempt to cover their tracks? A) Erasing the syslog file securely B) Changing or forging syslog entries C) Clearing specific syslog entries D) Clearing the syslog file	D. The attacker issued attempted to overwrite the /var/log/syslog file. If this command were successful, they would have overwritten all of the log's contents with a single space character. If the server writes its logs to a centralized Syslog server, the original logs would still be available for review. Additionally, this method does not securely erase the file, and it could be restored from a backup or even from the hard drive using forensic techniques. If the attacker wanted to erase the file securely, they should have used the "shred -zu /var/log/syslog" command. This would overwrite the area of the hard drive that contained the file with zeros for increase security.
Jason is conducting a penetration test against an organization's Windows network. This engagement aims to demonstrate what a trusted insider could do to the organization's network. The organization provided Jason with a corporate laptop and a standard user account as an entry-level employee. He was able to download his exploit (exploit.exe) and some programs from SysInternals to his desktop. He then enters the following commands into the command shell from this standard user account: -=-=-=-=-=- C:\Users\jason\Desktop> exploit.exe This program has been blocked by group policy. Contact your administrator to enable this program. C:\Users\jason\Desktop> accesschk.exe -uwcq "jason" *RW Apache C:\Users\jason\Desktop> sc config "Apache" binPath= "net localgroup administrators jason /add" C:\Users\jason\Desktop> sc stop "Apache" C:\Users\jason\Desktop> sc start "Apache" -=-=-=-=-=- Based on the output above, which of the fo	B. Some Windows services are run with SYSTEM privileges and may have been misconfigured by the administrator. In this case, Jason used the accesschk tool from SysInternals to find any writeable services that his user account could access. One was returned: Apache. He then stopped the service and rewrote the binary path loaded by the service to "net localgroup administrators jason /add", which will be run the next time the service is started. This will add Jason's user account (jason) to the administrators group. Next, he started the service, completing his privilege escalation through the use of writeable services.

An attacker was able to gain access to your organization's network closet while posing as an HVAC technician. While he was there, he installed a network sniffer in your switched network environment. The attacker now wants to sniff all of the packets in the network. What attack should he use? A) Fraggle B) MAC Flood C) Smurf D) Tear Drop	B. MAC flooding is a technique employed to compromise the security of switched network devices. The attack forcing legitimate MAC addresses out of the table of contents in the switch and forcing a unicast flooding behavior, potentially sending sensitive information to portions of the network where it is not normally intended to go. Essentially, since the switch table of contents is flooding with bad information, the switch could fail open and begin to act like a hub, broadcasting all the frames out of every port. This would allow the attacker to sniff all network packets since he is connected to one of those switch ports. A fraggle attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented TCP packets to a target machine. The Smurf attack is a distributed denial-of-service attack. Large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.
Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed many file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT? A) Network traffic analysis B) Network forensics C) Endpoint behavior analysis D) Endpoint forensics	D. An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. APTs usually send encrypted traffic so that they are harder to detect through network traffic analysis or network forensics. This means that you need to focus on the endpoints to detect an APT. Unfortunately, APTs are very sophisticated, so endpoint behavioral analysis is unlikely to detect them easily, so Sarah will need to conduct endpoint forensics as her most likely method to detect an APT and their associated infections on her systems.
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? A) nmap -sS B) nmap -O C) nmap -sT D) nmap -sX	C. The nmap TCP connect scan (-sT) is used when the SYN scan (-sS) is not an option. You should use the -sT flag when you d not have raw packet privileges on your workstation or if you are scanning an IPv6 network. This flag tells nmap to establish a connection with the target machine by issuing the connect system call instead of directly using an SYN scan. Normally, a fast scan using the -sS (SYN scan) flag is more often conducted, but it requires raw socket access on the scanning workstation. The -sX flag would conduct a Xmas scan where the FIN, PSH, and URG flags are used in the scan. The -O flag would conduct an operating system detection scan of the target system.
You have just run the following commands on your Linux workstation: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- DionTraining:~ root# ls Names.txt DionTraining:~ root# more Names.txt DION DIOn DIon Dion dion DionTraining:~ root# grep -i DION Names.txt =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Which of the following options would be included as part of the output for the grep command issued? (Select ANY that apply) A) DION B) DIOn C) Dion D) Dion E) dion	All. The grep (global search for regular expressions and print) is one of Linux's powerful search tools. The general syntax for the grep command is "grep [options] pattern [files]. The command searches within the specified files (in this case, the Names.txt file). When the command is issued with the -i optional flag, it treats the specified pattern as case insensitive. Therefore, all uppercase and lowercase variations of the word "DION" will be presented from the file and displayed as the command output. By default, grep uses case sensitivity, so "grep DION Names.txt" would only display the output as "DION" and ignore the other variations. As a cybersecurity analyst, grep is one of your most important tools. You can use regular expressions (regex) to quickly find indicators of compromise within your log files using grep.

A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output:
-=-=-=-=--=-=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=-
[443] [https-get-form] host: diontraining.com login: admin password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com login: admin password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com login: root password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com login: root password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com login: dion password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com login: dion password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com login: jason password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com login: jason password: C0mpT1@P@$$w0rd
-=-=-=-=--=-=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=-
What type of attack was most likely being atte

B. Password spraying refers to the attack method that takes many usernames and loops them with a single password. We can use multiple iterations using many different passwords, but the number of passwords attempted is usually low compared to the number of users attempted. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. In the scenario provided, only one or two attempts are being made to each username listed. This is indicative of a password spraying attack instead of a brute force attempt against a single user. Impersonation is the act of pretending to be another person for fraud. Credential stuffing is the automated injection of breached username/password pairs to gain user accounts access fraudulently. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account. The attacker can then hijack for their own purposes. Session hijacking exploits a valid computer session to gain unauthorized access to information or services in a computer system.

You are working as part of a penetration testing team during an engagement. A coworker just entered "Get-Service -DisplayName "Dion Training App" | Remove-Service" in PowerShell on the Windows server the team exploited. What action is your coworker performing with this command?

A) To enable persistance on the server
B) To enumerate the running services on the server
C) To remove persistance on the server
D) To shutdown the running service on the server

C. This scenario is using a chained command to remove persistence from a Windows server using PowerShell. The command entered removes a service named Dion Training App. The command uses Get-Service to get an object representing the Dion Training App service using the display name. The pipeline operator (|) pipes the object to Remove-Service, which removes the service. This will remove any persistence gained by running the Dion Training App, which is just a fictional service name used in this example to hide the penetration tester's persistence tools. This service could be named anything the penetration tester deems appropriate during the service's installation.

Tim is working to prevent any remote login attacks to the root account of a Linux system. What method would be the best option to stop attacks like this while still allowing normal users to connect using ssh?

A) Add an iptables rule blocking root logins
B) Add root to the subdoers group
C) Change sshd_config to deny root login
D) Add a network IPS rule to block root logins

C. Linux systems use the sshd (SSH daemon) to provide ssh connectivity. If Tim changes the sshd_config to deny root logins, it will still allow any authenticated non-root user to connect over ssh. The sshd service has a configuration setting that is named PermitRootLogin. If you set this configuration setting to no or deny, all root logins will be denied by the ssh daemon. If you didn't know about this setting, you could still answer this question by using the process of elimination. An iptables rule is a Linux firewall rule, and this would block the port for ssh, not the root login. Adding root to the sudoers group won't help either since the sudoers group allows users to login as root. If you have a network IPS rule to block root logins, the IPS would have to see the traffic being sent within the SSH tunnel. This is not possible since SSH connections are encrypted end-to-end by default. Therefore, the only possible right answer is to change the sshd_config setting to deny root logins.

Review the following packet captured at your NIDS:
-=-
23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq 1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc 482862734, length 125
-=-
After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host?

A) DENY TCP ANY HOST 71.168.10.45 EQ 3389
B) DENY IP HOST 71.168.10.45 ANY EQ 25

A. Since the question asks you to prevent unauthorized service access, we need to block port 3389 from accepting connections on 71.168.10.45 (the host). This option will deny ANY workstation from connecting to this machine (host) over the Remote Desktop Protocol service that is unauthorized (port 3389).

C) DENY IP HOST 86.18.10.3 EQ 3389
D) DENY TCP ANY HOST 86.18.10.3 EQ 25