CYSA

Study online at https://quizlet.com/_fi2pbp

In the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, security controls are categories into one of 18 families. What does a category of RA mean? Regular Access Regulatory Administrative Risk Assessment Reduced Administration	Risk Assessment
Which security control functional type is used to identify and record any attempted or successful intrusion? Detective Control Corrective Control Preventative Control Administrative Control	Detective Control A detective control is a a type of security control that acts during an incident to identify or record that it is happening. A detective control operates during the progress of an attack. Examples include logs and security cameras which are used to maintain a record of actions taken by an attacker.
Which of the following automatically combines multiple disparate sources of information together to form a complete picture of events for analysts to use during an incident response or when conducting proactive threat hunting? Machine Learning Deep Learning Data Enrichment Continuous integration	Data Enrichment When data enrichment is occurring, it could combine a threat intelligence feed with a log of NetFlow. This will allow the analyst to know if an IP address of interest is actually associated with a known APT. Machine learning and deep learning are forms of artificial intelligence that may be used to conduct data enrichment activities, but individually they are not sufficient to answer this question. Continuous integration is a software development method in which code updates are tested and committed to a development or build server/code repository rapidly, and is unrelated to this question.
In which phase of the security intelligence cycle is input collected from intelligence producers and consumers to improve the implementation of intelligence requirements? Feedback Analysis Dissemination Collection	Feedback The final phase of the security intelligence cycle is feedback and review, which utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases as the life cycle is developed.
Which of the following is an example of an open-source intelligence feed? IBM X-Force Exchange Recorded Future FireEye Malware Information Sharing Project	Malware Information Sharing Project The Malware Information Sharing Project, or MISP, is an open-source intelligence feed. Other popular open-source intelligence feeds are AT&T Security (Alien Vault Open Threat Exchange), Spamhaus, SANS ISC Suspicious Domains, VirusTotal, and NCAS by US0CERT. Closed-source or proprietary intelligence sources include IBM X-Force Exchange, Recorded Future, and FireEye.
Which type of threat will patches NOT effectively combat as a security control? Zero-day attacks Known vulnerabilities Discovered software bugs Malware with defined indicators of compromise	Zero-day Attacks Zero-day attacks have no known fix, so patches will not correct them. A zero-day vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). If a discovered software bug or known vulnerability is found, there is normally a patch or mitigation available for it. If a piece of malware has well-defined indicators of compromise, a patch or signature can be created to defend against it, as well.
Which analysis framework provides the most explicit detail regarding how to mitigate or detect a given threat?	MITRE ATT&CK framework The MITRE ATT&CK framework provides explicit pseudo-code examples for how to detect or mitigate a given threat within a network and ties specific behaviors back to individual actors. The

Diamond Model of Intrusion Analysis MITRE ATT&CK framework OpenIOC Lockheed Martin cyber kill chain	Diamond Model provides an excellent methodology for communicating cyber events and allowing an analyst to implicitly derive mitigation strategies. The Lockheed Martin cyber kill chain provides a general life cycle description of how attacks occur but does not deal with the specifics of how to mitigate. OpenIOC contains a depth of research on APTs but does not integrate the detections and mitigation strategy.
What is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial TTPs within a network or system called? Incident response Penetration testing Threat hunting Information assurance	Threat Hunting Threat hunting is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial TTPs within a network or system.
What technique is an attacker using if they are reviewing data and publicly available information to gather intelligence about the target organization without scanning or other technical information gathering activities? Passive Recon Active Scanning Vulnerability Scanning Patch Management	Passive Recon Passive reconnaissance combines publicly available data from a variety of sources about an organization and does not use active scanning or data gathering methods.
A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URL, https://www.google.com/search?q=*%40diontraining.com. Which of the following is true about the results of this search? Returns no useful results for an attacker Returns all web pages containing the text diontraining.com Returns all web pages containing an email address affiliated with diontraining.com Returns all web pages hosted at diontraining.com	Returns all web pages containing an email address affiliated with diontraining.com Google interprets this statement as <anything>@diontraining.com and understands that the user is searching for email addresses since %40 is the hex code for the @ symbol. The * is a wild card character meaning that any text could be substituted for the * in the query. This type of search would provide an attacker with a list of email addresses associated with diontraining.com, and therefore could be used as part of a spear-phishing campaign.
A company's NetFlow collection system can handle up to 2 Gbps. Due to excessive load, this has begun to approach full utilization at various times of the day. If the security team does not have additional money in their budget to purchase a more capable collector, which of the following options could they use to collect useful data? Enable QoS Enable NetFlow compression Enable sampling of the data Enable full packet capture	Enable sampling of the data The organization should enable sampling of the data collected. Sampling can help them to capture network flows that could be useful without collecting everything passing through the sensor. This reduces the bottleneck of 2 Gbps and still provide useful information.
When using tcpdump, which option or flag would you use to record the ethernet frames during a packet capture? -n -nn -e -X	-e The -e option includes the ethernet header during packet capture. The -n flag will show the IP addresses in numeric form. The -nn option shows IP addresses and ports in numeric format. The -X option will capture the packet's payload in hex and ASCII formats.
A cybersecurity analyst is attempting to perform an active reconnaissance technique to audit their company's security controls. Which DNS assessment technique would be classified as active? A DNS forward or reverse loop A zone transfer A whois query Using maltego	zone transfer DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. DNS zone transfers are an active technique.

While performing a vulnerability scan, Christina discovered an administrative interface to a storage system is exposed to the internet. She looks through the firewall logs and attempts to determine whether any access attempts have occurred from external sources. Which of the following IP addresses in the firewall logs would indicate a connection attempt from an external source? 10.15.1.100 192.186.1.100 172.16.1.100 192.168.1.100	192.186.1.100 This question is testing your ability to determine if an IP address is a publicly routable IP (external connection) or private IP (internal connection). During your CompTIA A+, Network+, and Security+ studies, you should have learned that private IP addresses are either 10.x.x.x, 172.16-31.x.x, or 192.168.x.x. All other IP addresses are considered publicly routable over the internet (except localhost and APIPA addresses). Therefore, the answer must be 192.186.1.100, since it is not a private IP address.
Evaluate the following log entry: -= Jan 11 05:52:56 lx1 kernel: iptables INPUT drop IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=3988 DF PROTO=TCP SPT=2583 DPT=23 WINDOW=64240 RES=0x00 SYN URGP=0 -= Based on this log entry, which of the following statements is true? MAC filtering is enabled on the firewall An attempted connection to the ssh service was prevented The packet was blocked inbound to the network Packets are being blocked inbound to and outbound from the network	The packet was blocked inbound to the network Firewall log formats will vary by vendors, but this example is a commonly used format from the Linux iptable firewall tool. This log starts with the date and time of the event and provides some key pieces of information. For example, the word "drop" shows the action this log entry recorded. In this case, the firewall dropped a packet due to an ACL rule being applied. Also, you can see that the packet was detected on the inbound connection over eth0, so we know that packets are being scanned and blocked when they are headed inbound to the network.
You are reviewing a rule within your organization's IDS. You see the following output: -= alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any msg: "BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt"; flow: to_client,established; file_data; content:"recordset"; offset:14; depth:9; content:".CacheSize"; distance:0; within:100; pcre:"/CacheSize\s*=\s*/"; byte_test:10,>,0x3ffffffe,0,relative,string; max-detect-ips drop, service http; reference:cve,2016-8077; classtype: attempted-user; sid:65535;rev:1; -= Based on this rule, which of the following malicious packets would this IDS alert on? An inbound malicious TCP packet Any outbound malicious packets An outbound malicious TCP packet Any inbound malicious packets	An inbound malicious TCP packet The rule header is set to alert only on TCP packets based on the first line of this IDS rule. The flow condition is set as "to_client,established", which means that only inbound traffic will be analyzed against this rule and only inbound traffic for connections that are already established. Therefore, this rule will alert on an inbound malicious TCP packet only when the packet matches all the conditions listed in this rule. This rule is an example of a Snort IDS rule. For the exam, you do not need to be able to create your own IDS rules, but you should be able to read them and pick out data.
Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices? Installation of anti-virus tools Use of a host-based IDS or IPS Implement endpoint protection platforms User and entity behavior analytics	User and entity behavior analytics Since ICS, SCADA and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, the use of user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily dependent

	on advanced computing techniques like artificial intelligence and machine learning.
You are conducting an investigation on a suspected compromise. You have noticed several files that you don't recognize. How can you quickly and effectively check if the files have been infected with malware? Submit the files to an open-source intelligence provider like Virus-Total Disassembly the files and conduct static analysis on them using IDA Pro Run the Strings tool against each file to identify common malware identifiers Scan the files using a local anti-virus/anti-malware engine	Submit the files to an open-source intelligence provider like Virus-Total The best option is to submit them to an open-source intelligence provider like VirusTotal. VirusTotal allows you to quickly analyze suspicious files and URLs to detect types of malware. It then automatically shares them with the security community, as well. Disassembly and static analysis would require a higher level of knowledge and more time to complete. Running the Strings tool can help identify text if the code is not encoded in a specific way within the malware, but you have to know what you are looking for, such as a malware signature.
Your company just launched a new invoicing website for use by your five largest vendors. You are the cybersecurity analyst and have been receiving numerous phone calls that the webpage is timing out and the website overall is performing slowly. You have noticed that the website received three million requests in just 24 hours and the service has now become unavailable for use. What do you recommend should be implemented to restore and maintain the availability of the new invoicing system? Intrusion Detection System VPN Whitelisting MAC filtering	Whitelisting By implementing whitelisting of the authorized IP addresses for the five largest vendors, they will be the only ones who will be able to access the webserver. This can be done by creating rules in the Access Control List (ACL) to deny ALL other users except these five vendors, thereby dropping a large number of requests from any other IP addresses, such as those from an attacker.
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? Configuration management systems DMARC and DKIM SIEM systems Log files	DMARC and DKIM Vulnerability scans should never take place in a vacuum. Analysts should correlate scan results with other information sources, including logs, SIEM systems, and configuration management systems. DMARC (domain-based message authentication, reporting, and conformance) and DKIM (domain keys identified mail) are configurations that are performed on a DNS server to verify whether email being sent by a third-party is verified to send it on behalf of the organization.
You just received a notification that your company's email servers have been blacklisted due to reports of spam originating from your domain. What information do you need to start investigating the source of the spam emails? Firewall logs showing the SMTP connections The SMTP audit log from his company's email server The full email header from one of the spam messages Network flows for the DMZ containing the email servers	The full email header from one of the spam messages You should first request a copy of one of the spam messages that include the full email header. By reading through the full headers of one of the messages, you can determine where the email originated from, whether it was from your email system or if it was external, and if it was a spoofed email or a legitimate email. Once this information has been analyzed, you can then continue your analysis further based on those findings, whether that be analyzing your email server, the firewalls, or other areas of concern. This was discussed in Lecture 57: Email Header Analysis (OBJ 3.1)
You are a cybersecurity analyst who has been given the output from a system administrator's Linux terminal. Based on the output provided, which of the following statements is correct? -=- BEGIN OUTPUT ———————--------- # nmap win2k16.local Nmap scan report for win2k16 (192.168.2.15) Host is up (0.132452s latency) Not shown: 997 closed ports	

PORT STATE SERVICE 22/tcp open ssh 80/tcp open http # nc win2k16.local 80 220 win2k16.local DionTraining SMTP Server (Postfix/2.4.1) # nc win2k16.local 22 SSH-2.0-OpenSSH_7.2 Debian-2 # ———————--------- END OUTPUT -=- Your email server is running on a non-standard port Your email server has been compromised Your organization has a vulnerable version of the SSH server software installed Your web server has been compromised	Your email server is running on a non-standard port As shown in the output of the nmap scans, only two standard ports are being utilized: 22 (SSH) and 80 (HTTP). But, when netcat is run against port 80, the banner that is provided shows the SMTP server is running on port 80. SMTP is normally run on port 25 by default, so running it on port 80 means your email server (SMTP) is running on a non-standard port.
A cybersecurity analyst is conducting proactive threat hunting on a network by correlating and search 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? Data exfiltration Unauthorized software Processor consumption Irregular peer-to-peer communication	Unauthorized Software This is a difficult question, but you should see a keyword in the query, "mimikatz". Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs, and Kerberos tickets. Other useful attacks it enables are pass-the-hash, pass-the-ticket, or building Golden Kerberos tickets. This makes post-exploitation lateral movement within a network easy for attackers. It is definitely considered unauthorized software and should be immediately alerted upon if discovered in your network.
While studying for your CompTIA CySA+ course at Dion Training, you decided you want to install a SIEM to collect data on your home network and its systems. You do not want to spend any money purchasing a license, so you decide to use an open-source option instead. Which of the following SIEM solutions utilize an open-source licensing model? Splunk QRadar OSSIM ArcSight	OSSIM OSSIM is an open-source SIEM developed by AlienVault. It is capable of pulling information together from a wide variety of sources. ArcSight, Qradar, and Splunk are all proprietary, commercially licensed SIEM solutions.
You are conducting an intensive vulnerability scan to detect which ports might be open to exploitation. During the scan, one of the network services becomes disabled and causes an impact on the production server. Which of the following sources of information would provide you with the most relevant information for you to use in determining which network service was interrupted and why? Syslog Network mapping Firewall logs NIDS	Syslog The syslog server is a centralized log management solution. By looking through the logs on the syslog server, the technician could determine which service failed on which server, since all the logs are retained on the syslog server from all of the network devices and servers.
Learn more about regex	https://www.regexr.com
Alexa is an analyst for a large bank that has offices in multiple states. She wants to create an alert to detect when an employee	

from one bank office logs into a workstation located at an office in another state. What type of detection and analysis is Alexa configuring? Trend Anomaly Heuristic Behavior	This is an example of behavior-based detection. Behavior-based detection (or statistical- or profile-based detection) means that the engine is trained to recognize baseline traffic or expected events associated with a user account or network device. Anything that deviates from this baseline (outside a defined level of tolerance) generates an alert.
You have been asked to review the SIEM event logs for suspected APT activity. You have been given several indicators of compromise, such as a list of domain names and IP addresses. What is the BEST action to take in order to analyze the suspected APT activity? Use the IP addresses to search through the event logs Analyze the trends of the events while manually reviewing them to see if any indicators match Create an advanced query that includes all of the indicators and review any matches Scan for vulnerabilities with exploits known to previously have been used by an APT	B If you only searched through the event logs using the IP addresses, this would not be sufficient as many APTs hide their activity by compromising and using legitimate networks and their IP addresses. If you only use the IP addresses to search the event logs, you would miss any events that correlated only to the domain names. If you create an advanced query will all of the indicators, your search of the event logs will find nothing because no single event will include all of these IPs and domain names. Finally, while scanning for vulnerabilities is a good practice, it would not be effective.
Consider the following file called firewall.log that contains 53,682 lines that logged every connection going into and out of this network. The log file is in the following data format, as shown below with the first two lines of the log file: -= DATE,FACILITY,CHAIN,IN,SRC,DST,LEN,TOS,PREC,TTL,ID,PROTO,SPT,DPT Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0,10.1.0.102,10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,23 -= Which of the following commands would display all of the lines from the firewall.log file that contain the destination IP address of 10.1.0.10 and a destination port of 23? grep "10.1.0.10," firewall.log | grep "23$" grep "10\.1\.0\.10\," firewall.log \| grep "23" grep "10\.1\.0\.10\," firewall.log \| grep "23$" grep "10.1.0.10," firewall.log | grep "23"	C When using the dot in the IP addresses, you must remember to escape this character or else grep treats it as a special character in a regular expression that is treated as any character (except a line break). By adding the \ before the dot (\.), grep treats it simply as a dot or period. You must also escape the comma for it to be processed properly. The $ after the port number is used to indicate that the number should only be counted as a match if it is at the end of the line. This ensures that we only return the destination ports (DPT) matching 23 and not the source port (SPT).
You are the first forensic analyst to arrive on the scene of a data breach. You have been asked to begin evidence collection on the server while waiting for the rest of your team to arrive. Which of the following evidence should you capture first? Image of the server's SSD L3 cache Backup tapes ARP cache	L3 Cache When collecting evidence, you should always follow the order of volatility. This will allow you to collect the most volatile evidence (most likely to change) first, and the least volatile (least likely to change) last. You should always begin the collection with the CPU registers and cache memory (L1/L2/L3/GPU). The contents of system memory (RAM), including a routing table, ARP cache, process tables, kernel statistics, and temporary file systems/swap space/virtual memory. Next, you would move onto the collection of data storage devices like hard drives, SSDs, and flash memory devices.
You are conducting a forensic analysis of a hard disk and need to access a file that appears to have been deleted. Upon analysis, you have determined that data fragments from the file exist scattered across the unallocated and slack space of the drive. Which technique could you use to recover the data?	Carving File carving is the process of extracting data from an image when that data has no associated file system metadata. A file-carving tool analyzes the disk at sector/page level and attempts to piece together data fragments from unallocated and slack space to

Hashing Recovery Overwrite Carving	reconstruct deleted files, or at least bits of information from deleted files. File carving depends heavily on file signatures or magic numbers—the sequence of bytes at the start of each file that identifies its type.
What information should be recorded on a chain of custody form during a forensic investigation? The list of individuals who made contact with files leading to the investigation The list of former owners/operators of the workstation involved in the investigation Any individual who worked with evidence during the investigation The law enforcement agent who was first on the scene	Any individual who worked with evidence during the investigation Chain of custody forms are forms that list every person who has worked with or who has made contact with the evidence that is a part of an investigation. These forms record every action taken by each individual in possession of the evidence. Depending on the organization's procedures, manipulation of evidence may require an additional person to act as a witness to verify whatever action is being taken. While the chain of custody would record who initially collected the evidence, it does not have to record who was the first person on the scene (if that person didn't collect the evidence).