Vendor: CompTIA

Exam Code: SY0-601

Exam Name: CompTIA Security+ Certification Exam

Version: DEMO

QUESTION 1
A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

A. Rainbow table attack
B. Password spraying
C. Logic bomb
D. Malware bot

Answer: B
Explanation:
Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

QUESTION 2
A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back end server resources and has highlighted that session persistence is not important for the applications running on the back end servers. Which of the following would BEST meet the requirements?

A. Reverse proxy
B. Automated patch management
C. Snapshots
D. NIC teaming

Answer: A
Explanation:
A reverse proxy would be the best solution for increased scalability and flexibility for back end infrastructure.

QUESTION 3
Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

A. Version control
B. Continuous monitoring
C. Stored procedures
D. Automation

Answer: A
Explanation:
Version control, also known as source control, is the process of tracking and managing changes to files over time. VCS -- version control systems -- are software tools designed to help teams work in parallel.
https://www.perforce.com/blog/vcs/what-is-version-control

QUESTION 4
Which of the following describes a social engineering technique that seeks to exploit a person's

sense of urgency?

A. A phishing email stating a cash settlement has been awarded but will expire soon
B. A smishing message stating a package is scheduled for pickup
C. A vishing call that requests a donation be made to a local charity
D. A SPIM notification claiming to be undercover law enforcement investigating a cybercrime

Answer: A
Explanation:
Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or%20fear%20in%20victims.

QUESTION 5
A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certificate the company should implement?

A. Subject alternative name
B. Wildcard
C. Self-signed
D. Domain validation

Answer: B
Explanation:
Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.'
For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.
A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.
https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/

QUESTION 6
A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. A bot
B. A fileless virus

C. A logic bomb
D. A RAT

Answer: D
Explanation:
Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

QUESTION 7
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.
C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.

Answer: D
Explanation:
A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non- credentialed scan on the network and finds that there are three missing patches. The scan does not provide many details on these missing patches. The administrator installs the missing patches to keep the systems up to date as they can only operate on the information produced for them.

QUESTION 8
While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method.
Which of the following would BEST detect a malicious actor?

A. Utilizing SIEM correlation engines
B. Deploying Netflow at the network border
C. Disabling session tokens for all sites
D. Deploying a WAF for the web server

Answer: A
Explanation:
The initial compromise was a malicious request on a web server. Moments later the token created with SSO was used on another service, the question does not specify what type of service.
Deploying a WAF on the web server will detect the attacker but only on that server. If the attacker issues the same malicious request to get another SSO token correlating that event with using that SSO token in other services would allows to detect the malicious activity.

QUESTION 9
As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

A. User behavior analysis
B. Packet captures
C. Configuration reviews
D. Log analysis

Answer: D
Explanation:
Configuration review is part of the vulnerability scan. Vulnerability scan can produce false positives, which is why its effectiveness can be enhanced by log reviews to see whether an identified vulnerability is in fact valid.

QUESTION 10
A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple login entries with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh
suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of the following is the MOST likely attack conducted on the environment?

A. Malicious script
B. Privilege escalation
C. Domain hijacking
D. DNS poisoning

Answer: A
Explanation:
A-Malicious scripts are fragments of code that have been modified by threat actors for nefarious purposes. Cyber threat actors hide them in legitimate websites, third-party scripts, and other places to compromise the security of client-side web applications and webpages.

QUESTION 11
Which of the following environments minimizes end user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code in an operationally representative environment?

A. Staging
B. Test
C. Production
D. Development

Answer: A
Explanation:
A staging environment is used to validate code that will be deployed. I have seen you providing answers with no context behind them and being wrong. You need to stop that.

QUESTION 12

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases.
Which of the following attacks took place?

A. On-path attack
B. Protocol poisoning
C. Domain hijacking
D. Bluejacking

Answer: A
Explanation:
On-path (MTM) - attacker was eavesdropping on the communications, spoofed the IP of the shopping site that the victim thought was legit, a purchase was attempted, credit info intercepted.

QUESTION 13
The Chief Information Security Officer warns lo prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP
B. USB data blocker
C. USB OTG
D. Disabling USB ports

Answer: B
Explanation:
Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice- jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point.

QUESTION 14
Which of the following employee roles is responsible for protecting an organization's collected personal information?

A. CTO
B. DPO
C. CEO
D. DBA

Answer: B
Explanation:
Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.

QUESTION 15
Which of the following control types is focused primarily on reducing risk before an incident occurs?

A. Preventive

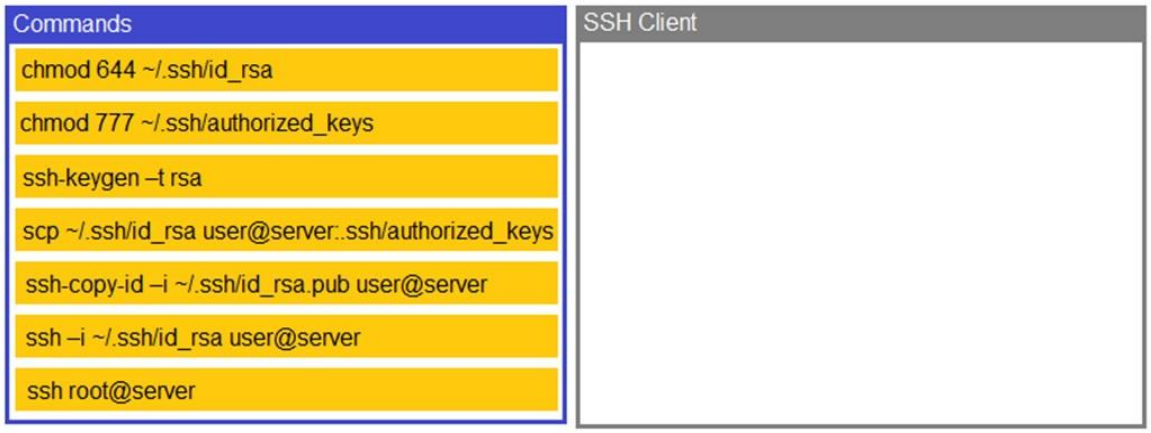
B. Deterrent
C. Corrective
D. Detective

Answer: A
Explanation:
A preventive control is designed to be implemented prior to a threat event and reduce and/or avoid the likelihood and potential impact of a successful threat event.

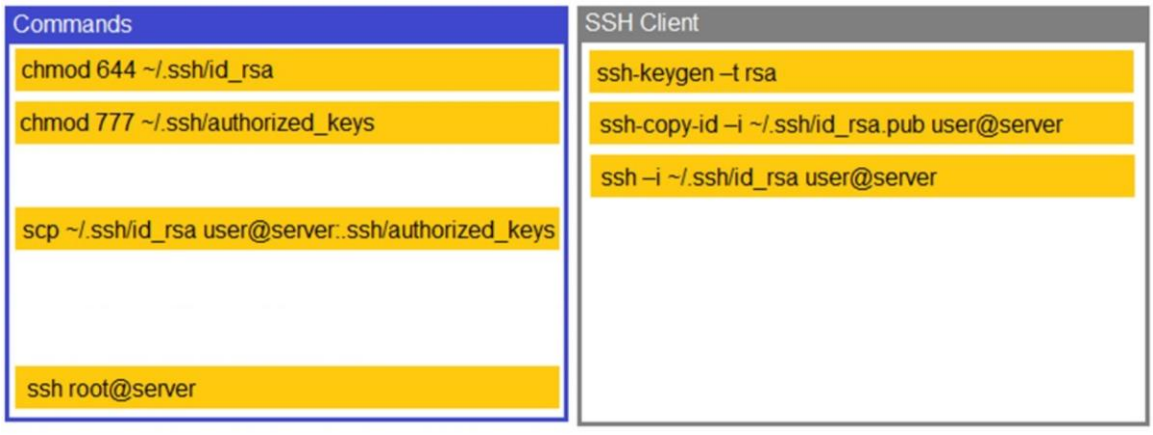
QUESTION 16
Drag and Drop Question

A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



Explanation:
1. ssh-keygen -t rsa (creating the key-pair)

2. ssh-copy-id -i /.ssh/id_rsa.pub user@server (copy the public-key to user@server)
3. ssh -i ~/.ssh/id_rsa user@server (login to remote host with private-key)

QUESTION 17
During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the Internet. The penetration tester stops the test to inform the client of the findings. Which of the following should be the client's NEXT step to mitigate the issue?

A. Conduct a full vulnerability scan to identify possible vulnerabilities.
B. Perform containment on the critical servers and resources
C. Review the firewall and identify the source of the active connection.
D. Disconnect the entire infrastructure from the Internet

Answer: B
Explanation:
Perform containment on the critical servers and resources -> Isolation or containment is the first thing to do after an incident has been discovered.

QUESTION 18
During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics
B. Dump files
C. Bandwidth monitors
D. Protocol analyzer output

Answer: A
Explanation:
User behavior analytics
User behavior analytics is a cybersecurity process about detection of insider threats, targeted attacks, and financial fraud that tracks a system's users. UBA looks at patterns of human behavior, and then analyzes them to detect anomalies that indicate potential threats.

QUESTION 19
A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framework
D. ISO 27002

Answer: D
Explanation:

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization and by the International Electrotechnical Commission, titled Information technology - Security techniques ?Code of practice for information security controls.

QUESTION 20
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. laC
B. MSSP
C. Containers
D. SaaS

Answer: A
Explanation:
Infrastructure as Code
Infrastructure as code is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

QUESTION 21
A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools, if available on the server, will provide the MOST useful information for the next assessment step?

A. Autopsy
B. Cuckoo
C. Memdump
D. Nmap

Answer: D
Explanation:
Memdump
A display or printout of all or selected contents of RAM. After a program abends (crashes), a memory dump is taken in order to analyze the status of the program. The programmer looks into the memory buffers to see which data items were being worked on at the time of failure.

Nmap
Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

QUESTION 22
Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft
B. Data loss

C. Data exfiltration
D. Reputation

Answer: C
Explanation:
Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft.

QUESTION 23
A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing
B. Use a web vulnerability scanner
C. Use static code analysis
D. Use a penetration-testing OS

Answer: C
Explanation:
Fuzzing
Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.
Static program analysis
Static program analysis is the analysis of computer software performed without executing any programs, in contrast with dynamic analysis, which is performed on programs during their execution.
What is static code analysis?
Static code analysis is a method of debugging by examining source code before a program is run. It's done by analyzing a set of code against a set (or multiple sets) of coding rules. ... This type of analysis addresses weaknesses in source code that might lead to vulnerabilities.
Penetration test
A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14