Exam Questions SY0-601

CompTIA Security+ Exam

https://www.2passeasy.com/dumps/SY0-601/

NEW QUESTION 1
A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

NEW QUESTION 2
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you are
E. Something you are
F. Something you can do

Answer: BE

NEW QUESTION 3
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

Answer: A

NEW QUESTION 4
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. IaaS
D. PaaS

Answer: B

NEW QUESTION 5
Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Answer: C

NEW QUESTION 6
Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM
B. CASB
C. UTM
D. DLP

Answer: D

NEW QUESTION 7
A security engineer is reviewing log files after a third discovered usernames and passwords for the organization’s accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in- the middle
B. Spear-phishing
C. Evil twin
D. DNS poising

Answer: D

NEW QUESTION 8
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 9
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Answer: D

NEW QUESTION 10
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Answer: AC

NEW QUESTION 10
Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log m to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE
B. VDI
C. GPS
D. TOTP
E. RFID
F. BYOD

Answer: BE

NEW QUESTION 15
An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

Answer: A

NEW QUESTION 16
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization’s vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

NEW QUESTION 20
A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

Answer: D

NEW QUESTION 23
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Answer: D

NEW QUESTION 28
Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. MOU
B. MTTR
C. SLA
D. NDA

Answer: C

NEW QUESTION 33
A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?

A. Netcat
B. Netstat
C. Nmap
D. Nessus

Answer: B

NEW QUESTION 38
A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholding
B. DLP rules on the terminal
C. An IP blacklist
D. Application whitelisting

Answer: D

NEW QUESTION 40
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth
B. Fingerprints
C. PIN
D. TPM

Answer: B

NEW QUESTION 44
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Answer: B

NEW QUESTION 49
A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST

prevent data? (Select TWO)

A. VPN
B. Drive encryption
C. Network firewall
D. File-level encryption
E. USB blocker
F. MFA

Answer: BE

NEW QUESTION 54
The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. Change control procedures
D. EDR reporting cycle

Answer: A

NEW QUESTION 58
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Answer: D

NEW QUESTION 59
A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.
Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

A. DoS
B. SSL stripping
C. Memory leak
D. Race condition
E. Shimming
F. Refactoring

Answer: AD

NEW QUESTION 64
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Answer: B

NEW QUESTION 69
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing
B. research the appropriate mitigation techniques in a vulnerability database
C. find the software patches that are required to mitigate a vulnerability
D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

NEW QUESTION 70
An organization’s help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

Answer: B

NEW QUESTION 75
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Answer: A

NEW QUESTION 76
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

Answer: B

NEW QUESTION 78
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

A. SDP
B. AAA
C. IaaS
D. MSSP
E. Microservices

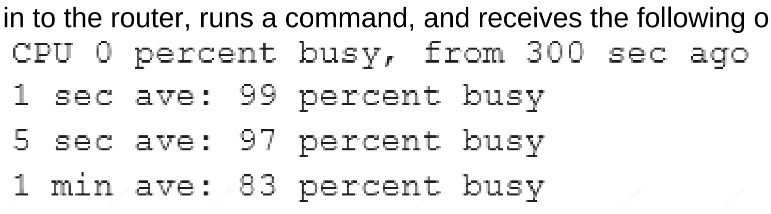
Answer: D

NEW QUESTION 81
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

A. A capture-the-flag competition
B. A phishing simulation
C. Physical security training
D. Baste awareness training

Answer: B

NEW QUESTION 82
A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:



```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

Answer: D

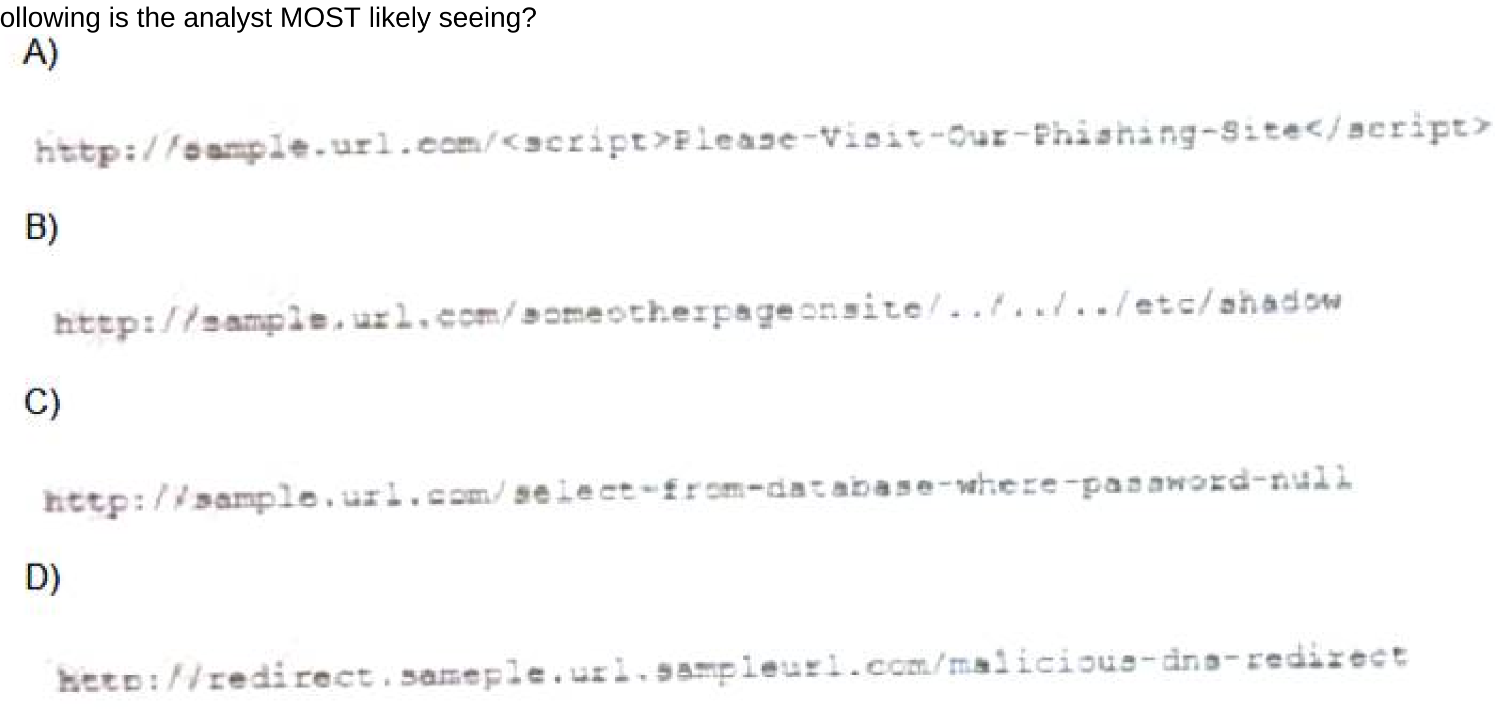
NEW QUESTION 86
A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

A. A malicious USB was introduced by an unsuspecting employee.
B. The ICS firmware was outdated
C. A local machine has a RAT installed.

D. The HVAC was connected to the maintenance vendor.

Answer: A

NEW QUESTION 89
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?



A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

A. Option A
B. Option B
C. Option C
D. Option D

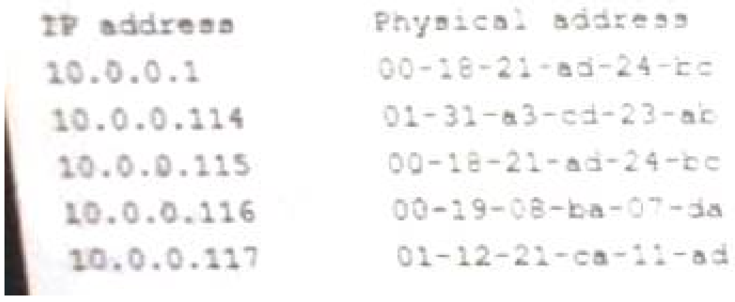
Answer: B

NEW QUESTION 94
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Answer: B

NEW QUESTION 95
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:



```
IP address        Physical address
10.0.0.1          00-18-21-ad-24-bc
10.0.0.114        01-31-a3-cd-23-ab
10.0.0.115        00-18-21-ad-24-bc
10.0.0.116        00-19-08-ba-07-da
10.0.0.117        01-12-21-ca-11-ad
```

Which of the following attacks has occurred?

A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Answer: E

NEW QUESTION 98
A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. OSINT
B. SIEM
C. CVSS

D. CVE

Answer: D

NEW QUESTION 99
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Answer: B

NEW QUESTION 100
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 105
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .t ar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 109
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 111
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Answer: C

NEW QUESTION 116
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

Answer: A

NEW QUESTION 120
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF

B. RPO
C. RTO
D. MTTR

Answer: C

NEW QUESTION 123
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Answer: C

NEW QUESTION 124
A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmapn
B. Heat maps
C. Network diagrams
D. Wireshark

Answer: C

NEW QUESTION 127
A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization’s network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A table exercise
B. NST CSF
C. MTRE ATT$CK
D. OWASP

Answer: A

NEW QUESTION 131
A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system
B. The system must be taken offline before a snapshot can be created
C. Checksum mismatches are invalidating the disk image
D. The swap file needs to be unlocked before it can be accessed

Answer: A

NEW QUESTION 134
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-601 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-601 Product From:

https://www.2passeasy.com/dumps/SY0-601/

Money Back Guarantee

SY0-601 Practice Exam Features:

* SY0-601 Questions and Answers Updated Frequently

* SY0-601 Practice Questions Verified by Expert Senior Certified Staff

* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year