SY0-601 Tested & Approved CompTIA Security+ Study Materials [Q50-Q70

SY0-601 Tested & Approved CompTIA Security+ Study Materials [Q50-Q70]

SY0-601 Tested & Approved CompTIA Security+ Study Materials
Validate your Skills with Updated CompTIA Security+ Exam Questions & Answers and Test Engine Q50. 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?

* Nmap
* cURL
* Netcat
* Wireshark

https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,packet%20data%20from%20a%20network.

Q51. A company is experiencing an increasing number of systems that are locking up on Windows startup. The security analyst clones a machine, enters into safe mode, and discovers a file in the startup process that runs Wstart.bat.

@echo off

:asdhbawdhbasdhbawdhb

```
start notepad.exe

start notepad.exe

start calculator.exe

start calculator.exe

goto asdhbawdhbasdhbawdhb
```

Given the file contents and the system&#8217;s issues, which of the following types of malware is present?
* Rootkit
* Logic bomb
* Worm
* Virus

Q52. 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?
* OSINT
* SIEM
* CVSS
* CVE

CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments.

Q53. Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user&#8217;s perspective against defined test cases? (Select TWO).
* Production
* Test
* Research and development
* PoC
* UAT
* SDLC

Q54. Acritical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?
* RAID0+1
* RAID 2
* RAID 5
* RAID 6

Q55. A security modern may have occurred on the desktop PC of an organization&#8217;s Chief Executive Officer (CEO) A duplicate copy of the CEO&#8217;s hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?
* Install a new hard drive in the CEO&#8217;s PC, and then remove the old hard drive and place it in a tamper-evident bag
* Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
* Remove the CEO&#8217;s hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
* Refrain from completing a forensic analysts of the CEO&#8217;s hard drive until after the incident is confirmed, duplicating the

hard drive at this stage could destroy evidence
Explanation

&#8220;To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker.&#8221; For purposes of knowing, https://security.opentext.com/tableau/hardware/details/t8u write blockers like this are the most popular hardware blockers

Q56. A malicious actor recently penetration a company&#8217;s network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?
* Security
* Application
* Dump
* Syslog
Explanation

Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them

https://www.digitalcitizen.life/view-contents-dump-file/

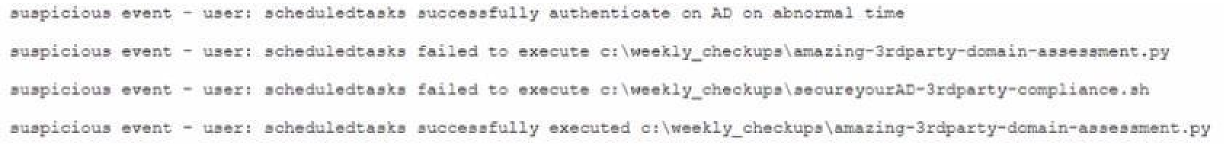
Q57. A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?
* SDP
* AAA
* IaaS
* MSSP
* Microservices
https://www.techtarget.com/searchitchannel/definition/MSSP

Q58. While checking logs, a security engineer notices a number of end users suddenly downloading files with the

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

https://www.howtogeek.com/362203/what-is-a-tar.gz-file-and-how-do-i-open-it/

Q59. A junior security analyst iss conducting an analysis after passwords were changed on multiple accounts without users&#8217; interaction. The SIEM have multiple logtn entnes 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 Ihe following is the MOST likely attack conducted on the environment?
* Malicious script
* Privilege escalation
* Doman hijacking
* DNS poisoning

Q60. A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall.

Which of the following would be the BEST option to remove the rules?
* # iptables -t mangle -X
* # iptables -F
* # iptables -Z
* # iptables -P INPUT -j DROP

Q61. A network administrator at a large organization Is reviewing methods to improve the security of the wired LAN Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?
* 802.1X utilizing the current PKI infrastructure
* SSO to authenticate corporate users
* MAC address filtering with ACLs on the router
* PAM for user account management

Q62. A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.
* validate the vulnerability exists in the organization&#8217;s network through penetration testing
* research the appropriate mitigation techniques in a vulnerability database
* find the software patches that are required to mitigate a vulnerability
* prioritize remediation of vulnerabilities based on the possible impact.

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Q63. Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?
* To avoid data leakage
* To protect surveillance logs
* To ensure availability
* To facilitate third-party access

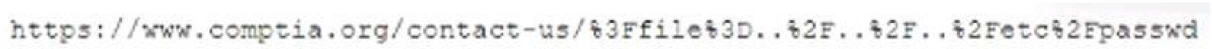
Q64. Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?
* Hashing
* Salting

- Integrity
- Digital signature

Q65. Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

- Transit gateway
- Cloud hot site
- Edge computing
- DNS sinkhole

Q66. A security analyst is reviewing web-application logs and finds the following log:



```
https://www.comptia.org/contact-us/%3Ffile%3D..%2F..%2F..%2Fetc%2Fpasswd
```

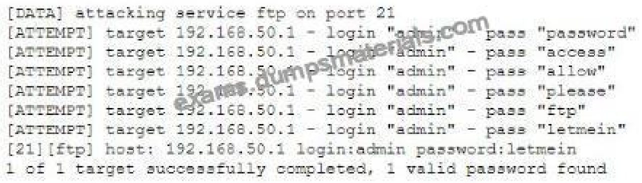
Which of the following attacks is being observed?

- Directory traversal
- XSS
- CSRF
- On-path attack

Q67. A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

- Password and security question
- Password and CAPTCHA
- Password and smart card
- Password and fingerprint
- Password and one-time token
- Password and voice

Q68. Given the following logs:



```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- Rainbow table
- Dictionary
- Password spraying
- Pass-the-hash

Q69. The SOC is reviewing processes and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- Updating the playbooks with better decision points

* Dividing the network into trusted and untrusted zones
* Providing additional end-user training on acceptable use
* Implementing manual quarantining of infected hosts

Q70. A systems analyst is responsible for generating a new digital forensics chain-of-custody form.

Which of the following should the analyst include in this documentation? (Choose two.)
* The order of volatility
* ACRC32 checksum
* The provenance of the artifacts
* The vendor&#8217;s name
* The date and time
* A warning banner

SY0-601 [Dec-2022 Newly Released SY0-601 Exam Questions For You To Pass:
https://www.dumpsmaterials.com/SY0-601-real-torrent.html]