- **Vendor: CompTIA**
- **Exam Code: SY0-601**
- **Exam Name: CompTIA Security+ Certification Exam**
- **New Updated Questions from Braindump2go**
- **(Updated in February/2022)**

QUESTION 497
A company wants to deploy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describe these systems?

A. DNS sinkholes
B. Honepots
C. Virtual machines
D. Neural network

Answer: A

QUESTION 498
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users PCs. Which of the following is the MOST likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.config instead of using the sshd.conf
D. Network services are no longer running on the NAS

Answer: C

QUESTION 499
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?

A. Hashing
B. Salting
C. Integrity
D. Digital signature

Answer: C

QUESTION 500
Users reported several suspicious activities within the last two weeks that resulted in several unauthorized transactions.

Upon investigation, the security analyst found the following:
- Multiple reports of breached credentials within that time period
- Traffic being redirected in certain parts of the network
- Fraudulent emails being sent by various internal users without their consent

Which of the following types of attacks was MOST likely used?

A. Replay attack
B. Race condition
C. Cross site scripting
D. Request forgeries

Answer: C

QUESTION 501
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 10.0.0.1

Internet Address      Physical Address
10.10.255.255         ff-ff-ff-ff-ff-ff
10.0.0.1              aa-aa-aa-aa-aa-aa
10.0.0.254            aa-aa-aa-aa-aa-aa
224.0.0.2             01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding

Answer: A

QUESTION 502
A company's cybersecurity department is looking for a new solution to maintain high availability. Which of the following can be utilized to build a solution? (Select Two)

A. A stateful inspection
B. IP hashes
C. A round robin
D. A VLAN
E. A DMZ

Answer: DE

QUESTION 503
A user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is MOST likely cause of the infection?

A. The driver has malware installed and was refactored upon download to avoid detection.
B. The user's computer has a rootkit installed that has avoided detection until the new driver overwrote key files.
C. The user's antivirus software definition were out of date and were damaged by the

installation of the driver

D. The user's computer has been infected with a logic bomb set to run when new driver was installed.

Answer: B

QUESTION 504
Which of the following controls would BEST identify and report malicious insider activities?

A. An intrusion detection system
B. A proxy
C. Audit trails
D. Strong authentication

Answer: A

QUESTION 505
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host

Answer: B

QUESTION 506
A SOC is currently being outsourced. Which of the following is being used?

A. Microservices
B. SaaS
C. MSSP
D. PaaS

Answer: C

QUESTION 507
A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

A. Private cloud
B. Hybrid environment
C. Managed security service provider
D. Hot backup site

Answer: B

QUESTION 508
An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved Which of the following attacks MOST likely explains the behavior?

A. Birthday
B. Rainbow table
C. Impersonation
D. Whaling

Answer: D

QUESTION 509
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key

Answer: D

QUESTION 510
An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap.

```
PORT      STATE
21/tcp    filtered
22/tcp    open
23/tcp    open
443/tcp   open
```

Which of the following should the analyst recommend to disable?

A. 21/tcp
B. 22/tcp
C. 23/tcp
D. 443/tcp

Answer: A