- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in June/2020)**

QUESTION 993
A transitive trust:

A. is automatically established between a parent and a child.
B. is used to update DNS records.
C. allows access to untrusted domains.
D. can be used in place of a hardware token for logins.

Answer: A

QUESTION 994
A systems administrator wants to disable the use of usernames and passwords for SSH authentication and enforce key-based authentication. Which of the following should the administrator do NEXT to enforce this new configuration?

A. Issue a public/private key pair for each user and securely distribute a private key to each employee.
B. Instruct users on how to create a public/private key pair and install users' public keys on the server.
C. Disable the username and password authentication and enable TOTP in the sshd.conf file.
D. Change the default SSH port. enable TCP tunneling. and provide a pre-configured SSH client.

Answer: D

QUESTION 995
Which of the following would MOST likely be a result of improperly configured user accounts?

A. Resource exhaustion
B. Buffer overflow
C. Session hijacking
D. Privilege escalation

Answer: D

QUESTION 996
An organization is concerned about video emissions from users' desktops. Which of the following is the BEST solution to implement?

A. Screen filters
B. Shielded cables

C. Spectrum analyzers
D. Infrared detection

Answer: A

QUESTION 997
A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

```
Time: 12/25 0300
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

When examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("Click here for important information regarding your account!
http://externalip.com/account.php"); </script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.
B. Manually copy the <script> data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.
C. Implement a host-based firewall rule to block future events of this type from occurring.
D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

Answer: B

QUESTION 998
Which of the following encryption algorithms require one encryption key? (Select TWO).

A. MD5
B. 3DES
C. BCRYPT
D. RC4
E. DSA

Answer: BD

QUESTION 999
A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

Answer: A

QUESTION 1000
Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure

the data will not be removed remotely?

A. Air gap
B. Secure cabinet
C. Faraday cage
D. Safe

Answer: C

QUESTION 1001
Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain
B. Notoriety
C. Political expression
D. Corporate espionage

Answer: B

QUESTION 1002
Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. pivoting.
B. persistence.
C. active reconnaissance.
D. a backdoor.

Answer: B

QUESTION 1003
An organization discovers that unauthorized applications have been installed on company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected with malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.
B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.
C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.
D. Some advanced users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

Answer: B

QUESTION 1004
Which of the following is a valid multifactor authentication combination?

A. OTP token combined with password
B. Strong password and PIN combination
C. OTP token plus smart card
D. Presence detecting facial recognition

Answer: A

QUESTION 1005

A security analyst is investigating a call from a user regarding one of the websites receiving a `503: Service Unavailable` error. The analyst runs a `netstat-an` command to discover if the web server is up and listening. The analyst receives the following output:

```
TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

Answer: C