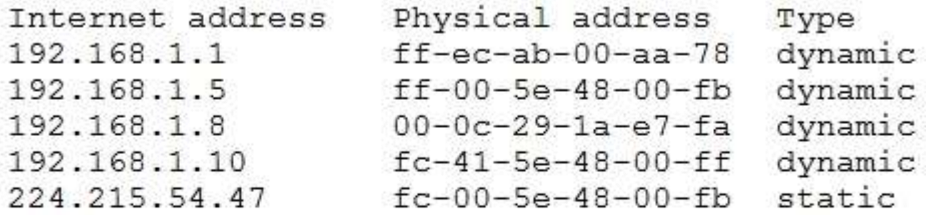
- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in Oct./2020)**

QUESTION 1215
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:



```
Internet address    Physical address    Type
192.168.1.1         ff-ec-ab-00-aa-78   dynamic
192.168.1.5         ff-00-5e-48-00-fb   dynamic
192.168.1.8         00-0c-29-1a-e7-fa   dynamic
192.168.1.10        fc-41-5e-48-00-ff   dynamic
224.215.54.47       fc-00-5e-48-00-fb   static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking

Answer: C

QUESTION 1216
A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing
B. Steganography tools
C. Protocol analyzer
D. Wireless scanner

Answer: A

QUESTION 1217
A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the disk of compromise while on foreign soil?

A. Disable firmware OTA updates.

B. Disable location services.
C. Disable push notification services.
D. Disable wipe.

Answer: B

QUESTION 1218
A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for Base64 encoded strings and applies the filter http.authbasic. Which of the following BEST describes what the analyst is looking for?

A. Unauthorized software
B. Unencrypted credentials
C. SSL certificate issues
D. Authentication tokens

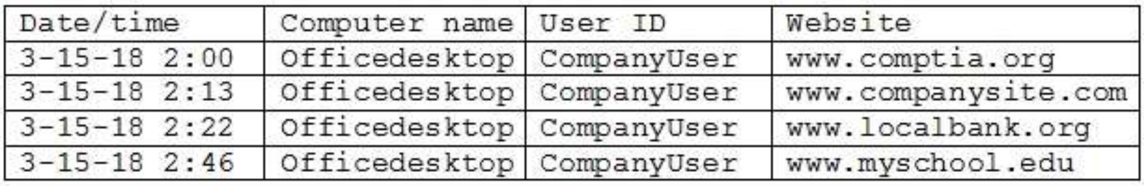
Answer: B

QUESTION 1219
Which of the following impacts are associated with vulnerabilities in embedded systems? (Choose two.)

A. Repeated exploitation due to unpatchable firmware
B. Denial of service due to an integrated legacy operating system.
C. Loss of inventory accountability due to device deployment
D. Key reuse and collision issues due to decentralized management.
E. Exhaustion of network resources resulting from poor NIC management.

Answer: AD

QUESTION 1220
Given the output:



Date/time	Computer name	User ID	Website
3-15-18 2:00	Officedesktop	CompanyUser	www.comptia.org
3-15-18 2:13	Officedesktop	CompanyUser	www.companysite.com
3-15-18 2:22	Officedesktop	CompanyUser	www.localbank.org
3-15-18 2:46	Officedesktop	CompanyUser	www.myschool.edu

Which of the following account management practices should the security engineer use to mitigate the identified risk?

A. Implement least privilege
B. Eliminate shared accounts.
C. Eliminate password reuse.
D. Implement two-factor authentication

Answer: B

QUESTION 1221
An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group.
B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.
C. Create two groups and ensure each group has representation from both the auditors and the

administrators so they can verify any changes that were made.

D. Assign file and folder permissions on an individual user basis and avoid group assignment altogether.

Answer: A

QUESTION 1222
Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Choose two.)

A. Accounting
B. Authentication
C. Auditing
D. Authorization
E. Non-repudiation

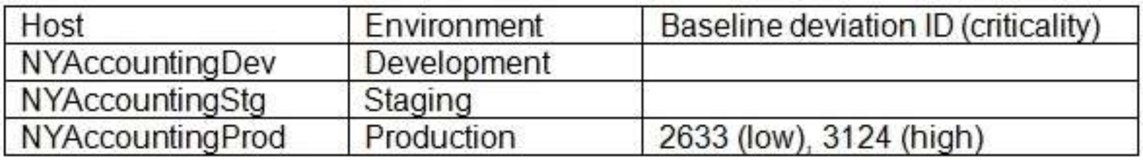
Answer: AC

QUESTION 1223
A datacenter engineer wants to ensure an organization's servers have high speed and high redundancy and can sustain the loss of two physical disks in an array. Which of the following RAID configurations should the engineer implement to deliver this functionality?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10
E. RAID 50

Answer: D

QUESTION 1224
An organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.
The application team receives a report with the following results:



Host	Environment	Baseline deviation ID (criticality)
NYAccountingDev	Development	
NYAccountingStg	Staging	
NYAccountingProd	Production	2633 (low), 3124 (high)

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate if the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?

A. Remediate 2633 and 3124 immediately.
B. Process a risk acceptance for 2633 and 3124.
C. Process a risk acceptance for 2633 and remediate 3124.
D. Shut down NYAccountingProd and investigate the reason for the different scan results.

Answer: C

QUESTION 1225
A company is having issues with intellectual property being sent to a competitor from its system. The information being sent is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop

the content from being sent?

A. Encryption
B. Hashing
C. IPS
D. DLP

Answer: D

QUESTION 1226
A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?

A. Implement promiscuous mode on the NIC of the employee's computer.
B. Install and configured a transparent proxy server.
C. Run a vulnerability scanner to capture DNS packets on the router.
D. Configure a VPN to forward packets to the technician's computer.

Answer: B

QUESTION 1227
A security administrator is adding a NAC requirement for all VPN users to ensure the connecting devices are compliant with company policy. Which of the following items provides the HIGHEST assurance to meet this requirement?

A. Implement a permanent agent.
B. Install antivirus software.
C. Use an agentless implementation.
D. Implement PKI.

Answer: A

QUESTION 1228
A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator implement?

A. WPS
B. PEAP
C. TKIP
D. PKI

Answer: A

QUESTION 1229
An organization is struggling to differentiate threats from normal traffic and access to systems. A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?

A. Web application firewall
B. SIEM
C. IPS
D. UTM
E. File integrity monitor

Answer: B

QUESTION 1230
The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.
B. a remote access policy.
C. multifactor authentication.
D. single sign-on.

Answer: A

QUESTION 1231
A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

Answer: B

QUESTION 1232
Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should a security administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS.
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

Answer: B

QUESTION 1233
A systems administrator wants to implement a secure wireless network requiring wireless clients to pre- register with the company and install a PKI client certificate prior to being able to connect to the wireless network. Which of the following should the systems administrator configure?

A. EAP-TTLS
B. EAP-TLS
C. EAP-FAST
D. EAP with PEAP
E. EAP with MSCHAPv2

Answer: B

QUESTION 1234
A systems administrator wants to replace the process of using a CRL to verify certificate validity. Which of the following would BEST suit the administrator's needs?

A. OCSP
B. CSR

C. Key escrow
D. CA

Answer: A

QUESTION 1235
Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the-browser
C. Spear phishing
D. Watering hole

Answer: A