CompTIA SY0-501 Exam

Volume: 88 Questions

Question: 1
A security analyst wishes to increase the security of an FTP server. Currently, all trails to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modem FTP client software. The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

A. Require the SFTP protocol to connect to the file server.

B. Use implicit TLS on the FTP server.

C. Use explicit FTPS for the connections.

D. Use SSH tunneling to encrypt the FTP traffic.

Answer: B

Question: 2
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords, The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select TWO)

A. The portal will function as an identity provider and issue an authentication assertion

B. The portal will request an authentication ticket from each network that is transitively trusted

C. The back-end networks will function as an identity provider and issue an authentication assertion

D. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store

E. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider

Answer: BC

Question: 3
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

A. CA public key

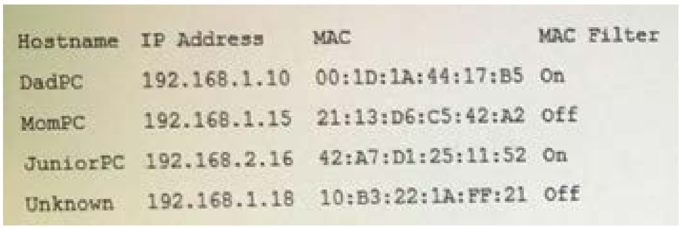
B. Server private key

C. CSR

D. OID

Answer: B

Question: 4
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system While attempting to determine if an unauthorized user is togged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.



Hostname	IP Address	MAC	MAC Filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.

B. Physically check each of the authorized systems to determine if they are togged onto the network.

C. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.

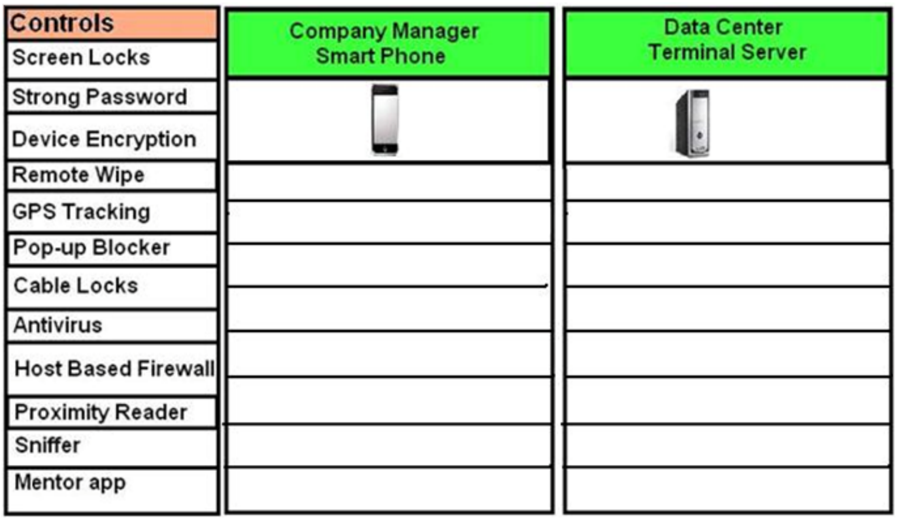
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Answer: C

Question: 5 DRAG DROP

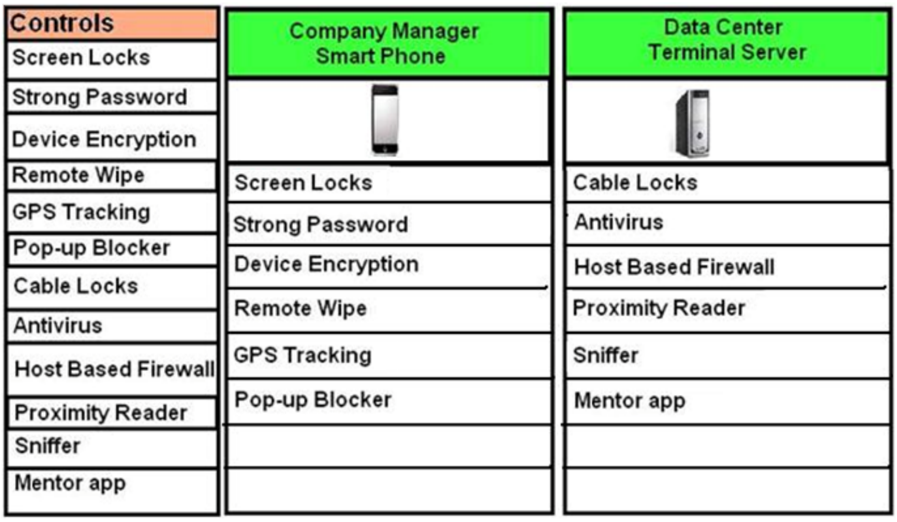
A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.

Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit.



Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up Blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mentor app		

Answer:



Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks	Screen Locks	Cable Locks
Strong Password	Strong Password	Antivirus
Device Encryption	Device Encryption	Host Based Firewall
Remote Wipe	Remote Wipe	Proximity Reader
GPS Tracking	GPS Tracking	Sniffer
Pop-up Blocker	Pop-up Blocker	Mentor app
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mentor app		

Question: 6

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.

B. SNMP data leaving the printer will not be properly encrypted.

C. An MITM attack can reveal sensitive information.

D. An attacker can easily inject malicious code into the printer firmware.

E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Answer: A

Question: 7

A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select TWO).

A. Generate an X 509-complaint certificate that is signed by a trusted CA.

B. Install and configure an SSH tunnel on the LDAP server.

C. Ensure port 389 is open between the clients and the servers using the communication.

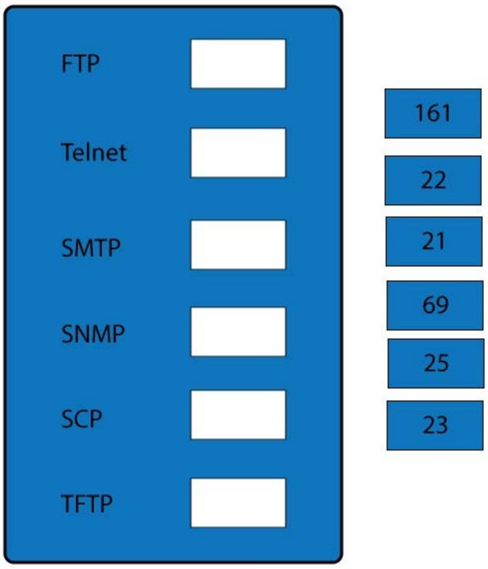
D. Ensure port 636 is open between the clients and the servers using the communication.

E. Remove the LDAP directory service role from the server.

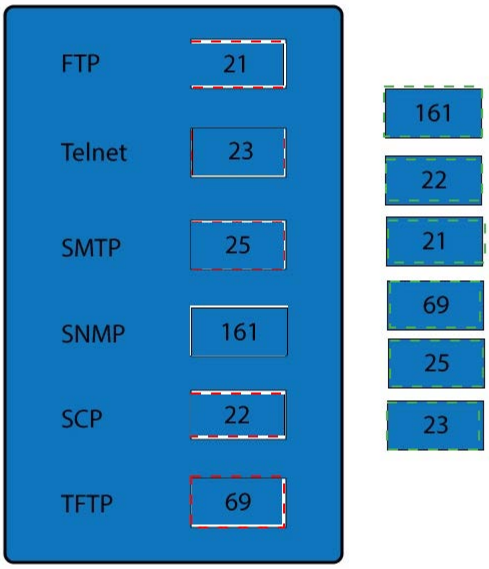
Answer: A,B

Question: 8 DRAG DROP

Drag and drop the correct protocol to its default port.



Answer:



Question: 9

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

A. SoC

B. ICS

C. IoT