SCP

Exam SC0-502

Security Certified Program (SCP)

Total Questions: 40

- QUESTION NO : 1

Now that you have Certkiller somewhat under control, you are getting ready to go home for the night. You have made good progress on the network recently, and things seem to be going smoothly. On your way out, you stop by the CEO's office and say good night. You are told that you will be meeting in the morning, so try to get in a few minutes early.

The next morning, you get to the office 20 minutes earlier than normal, and the CEO stops by your office, "Thanks for coming in a bit early. No problem really, I just wanted to discuss with you a current need we have with the network."

"OK, go right ahead." You know the network pretty well by now, and are ready for whatever is thrown your way.

"We are hiring 5 new salespeople, and they will all be working from home or on the road. I want to be sure that the network stays safe, and that they can get access no matter where they are."

"Not a problem," you reply. "I'll get the plan for this done right away."

"Thanks a lot, if you have any questions for me, just let me know."

You are relieved that there was not a major problem and do some background work for integrating the new remote users. After talking with the CEO more, you find out that the users will be working from there home nearly all the time, with very little access from on the road locations.

The remote users are all using Windows 2000 Professional, and will be part of the domain. The CEO has purchased all the remote users brand new Compaq laptops, just like the one used in the CEO's office, and which the CEO takes home each night; complete with DVD\CD-burner drives, built-in WNICs, 17" LCD widescreen displays, oversized hard drives, a gig of memory, and fast processing. 'I wish I was on the road to get one of those,' you think.

You start planning and decide that you will implement a new VPN Server next to the Web and FTP Server. You are going to assign the remote users IP Addresses: 10.10.60.100~10.10.60.105, and will configure the systems to run Windows 2000 Professional.

Based on this information, and your knowledge of the Certkiller network up to this point, choose the best solution for the secure remote user needs:}

A. You begin with configuring the VPN server, which is running Windows 2000 Server. You create five new accounts on that system, granting each of them the Allow Virtual Private Connections right in Active Directory Users and Computers. You then configure the range of IP Addresses to provide to the clients as: 10.10.60.100 through 10.10.60.105.

Next, you configure five IPSec Tunnel endpoints on the server, each to use L2TP as the protocol.

Then, you configure the clients. On each system, you configure a shortcut on the desktop to use to connect to the VPN. The shortcut is configured to create an L2TP IPSec tunnel to the VPN server.

The connection itself is configured to exchange keys with the user's ISP to create a tunnel between the user's ISP endpoint and the Certkiller VPN Server.

B. To start the project, you first work on the laptops you have been given. On each laptop, you configure the system to make a single Internet connection to the user's ISP.

Next, you configure a shortcut on the desktop for the VPN connection. You design the connection to use L2TP, with port filtering on outbound UDP 500 and UDP 1701. When a user double-clicks the desktop icon you have it configured to make an automatic tunnel to the VPN server.
On the VPN server, you configure the system to use L2TP with port filtering on inbound UDP 500 and UDP 1701. You create a static pool of assigned IP Address reservations for the five remote clients. You configure automatic redirection on the VPN server in the routing and remote access MMC, so once the client has connected to the VPN server, he or she will automatically be redirected to the inside network, with all resources available in his or her Network Neighborhood.
C. You configure the VPN clients first, by installing the VPN High Encryption Service Pack. With this installed, you configure the clients to use RSA, with 1024-bit keys. You configure a shortcut on the desktop that automatically uses the private\public key pair to communicate with the VPN Server, regardless of where the user is locally connected.
On the VPN Server, you also install the VPN High Encryption Service Pack, and configure 1024-bit RSA encryption. You create five new user accounts, and grant them all remote access rights, using Active Directory Sites and Services. You configure the VPN service to send the server's public key to the remote users upon the request to configure the tunnel. Once the request is made, the VPN server will build the tunnel, from the server side, to the client.
D. You decide to start the configuration on the VPN clients. You create a shortcut on the desktop to connect to the VPN Server. Your design is such that the user will simply double-click the shortcut and the client will make the VPN connection to the server, using PPTP. You do not configure any filters on the VPN client systems.
On the VPN Server, you first configure routing and remote access for the new accounts and allow them to have Dial-In access. You then configure a static IP Address pool for the five remote users. Next, you configure the remote access policy to grant remote access, and you implement the following PPTP filtering:
''Inbound Protocol 47 (GRE) allowed
''Inbound TCP source port 0, destination port 1723 allowed ''Inbound TCP source port 520, destination port 520 allowed ''Outbound Protocol 47 (GRE) allowed
''Outbound TCP source port 1723, destination port 0 allowed
''Outbound TCP source port 520, destination port 520 allowed
E. You choose to configure the VPN server first, by installing the VPN High Encryption Service Pack and the HISECVPN.INF built-in security template through the Security Configuration and Analysis Snap-In. Once the Service pack and template are installed, you configure five user accounts and a static pool of IP Addresses for each account.
You then configure the PPTP service on the VPN server, without using inbound or outbound filters - due to the protection of the Service Pack. You grant each user the right to dial into the server remotely, and move on to the laptops.
On each laptop, you install the VPN High Encryption Service Pack, to bring the security level of the laptops up to the same level as the VPN server. You then configure a shortcut on each desktop that controls the direct transport VPN connection from the client to the server.

Answer: D

- QUESTION NO : 2

Now that you have Certkiller somewhat under control, you are getting ready to go home for the night. You have made good progress on the network recently, and things seem to be going smoothly. On your way out, you stop by the CEO's office and say good night. You are told that you will be meeting in the morning, so try to get in a few minutes early.

The next morning, you get to the office 20 minutes earlier than normal, and the
CEO stops by your office, "Thanks for coming in a bit early. No problem really, I just wanted to discuss with you a current need we have with the network."

"OK, go right ahead." You know the network pretty well by now, and are ready for whatever is thrown your way.

"We are hiring 5 new salespeople, and they will all be working from home or on the road. I want to be sure that the network stays safe, and that they can get access no matter where they are."

"Not a problem," you reply. "I'll get the plan for this done right away."

"Thanks a lot, if you have any questions for me, just let me know."

You are relieved that there was not a major problem and do some background work for integrating the new remote users. After talking with the CEO more, you find out that the users will be working from there home nearly all the time, with very little access from on the road locations.

The remote users are all using Windows 2000 Professional, and will be part of the domain. The CEO has purchased all the remote users brand new Compaq laptops, just like the one used in the CEO's office, and which the CEO takes home each
night; complete with DVD\CD-burner drives, built-in WNICs, 17" LCD widescreen displays, oversized hard drives, a gig of memory, and fast processing. 'I wish I was on the road to get one of those,' you think.

You start planning and decide that you will implement a new VPN Server next to the Web and FTP Server. You are going to assign the remote users IP Addresses:
10.10.60.100~10.10.60.105, and will configure the systems to run Windows 2000 Professional.

Based on this information, and your knowledge of the Certkiller network up to this point, choose the best solution for the secure remote user needs:}

A. You begin with configuring the VPN server, which is running Windows 2000 Server.
You create five new accounts on that system, granting each of them the Allow Virtual Private Connections right in Active Directory Users and Computers. You then configure the range of IP Addresses to provide to the clients as: 10.10.60.100 through 10.10.60.105.
Next, you configure five IPSec Tunnel endpoints on the server, each to use L2TP as the protocol.

Then, you configure the clients. On each system, you configure a shortcut on the desktop to use to connect to the VPN. The shortcut is configured to create an L2TP IPSec tunnel to the VPN server. The connection itself is configured to exchange keys with the user's ISP to create a tunnel between the user's ISP endpoint and the Certkiller VPN Server.

B. To start the project, you first work on the laptops you have been given. On each laptop, you configure the system to make a single Internet connection to the user's ISP.

Next, you configure a shortcut on the desktop for the VPN connection. You design the connection to use L2TP, with port filtering on outbound UDP 500 and UDP 1701. When a user double-clicks the desktop icon you have it configured to make an automatic tunnel to the VPN server.

On the VPN server, you configure the system to use L2TP with port filtering on inbound UDP 500 and UDP 1701. You create a static pool of assigned IP Address reservations for the five remote clients. You configure automatic redirection on the VPN server in the routing and remote access MMC, so once the client has connected to the VPN server, he or she will automatically be redirected to the inside network, with all resources available in his or her Network Neighborhood.

C. You configure the VPN clients first, by installing the VPN High Encryption Service Pack. With this installed, you configure the clients to use RSA, with 1024-bit keys. You configure a shortcut on the desktop that automatically uses the private\public key pair to communicate with the VPN Server, regardless of where the user is locally connected.

On the VPN Server, you also install the VPN High Encryption Service Pack, and configure 1024-bit RSA encryption. You create five new user accounts, and grant them all remote access rights, using Active Directory Sites and Services. You configure the VPN service to send the server's public key to the remote users upon the request to configure the tunnel. Once the request is made, the VPN server will build the tunnel, from the server side, to the client.

D. You decide to start the configuration on the VPN clients. You create a shortcut on the desktop to connect to the VPN Server. Your design is such that the user will simply double-click the shortcut and the client will make the VPN connection to the server, using PPTP. You do not configure any filters on the VPN client systems.

On the VPN Server, you first configure routing and remote access for the new accounts and allow them to have Dial-In access. You then configure a static IP Address pool for the five remote users. Next, you configure the remote access policy to grant remote access, and you implement the following PPTP filtering:

''Inbound Protocol 47 (GRE) allowed

''Inbound TCP source port 0, destination port 1723 allowed ''Inbound TCP source port 520, destination port 520 allowed ''Outbound Protocol 47 (GRE) allowed

''Outbound TCP source port 1723, destination port 0 allowed

''Outbound TCP source port 520, destination port 520 allowed

E. You choose to configure the VPN server first, by installing the VPN High Encryption Service Pack and the HISECVPN.INF built-in security template through the Security Configuration and Analysis Snap-In. Once the Service pack and template are installed, you configure five user accounts and a static pool of IP Addresses for each account.

You then configure the PPTP service on the VPN server, without using inbound or outbound filters - due to the protection of the Service Pack. You grant each user the right to dial into the server

remotely, and move on to the laptops.
On each laptop, you install the VPN High Encryption Service Pack, to bring the security level of the laptops up to the same level as the VPN server. You then configure a shortcut on each desktop that controls the direct transport VPN connection from the client to the server.

Answer: A

- QUESTION NO : 3

For three years you have worked with Certkiller doing occasional network and security consulting. Certkiller is a small business that provides real estate listings and data to realtors in several of the surrounding states. The company is open for business Monday through Friday from9 am to 6 pm, closed all evenings and weekends. Your work there has largely consisted of advice and planning, and you have been frequently disappointed by the lack of execution and follow through from the full time staff.
On Tuesday, you received a call from Certkiller 's HR director, "Hello, I'd like to inform you that Red (the full time senior network administrator) is no longer with us, and we would like to know if you are interested in working with us full time."
You currently have no other main clients, so you reply, "Sure, when do you need me to get going?"
"Today," comes the fast and direct response. Too fast, you think. "What is the urgency, why can't this wait until tomorrow?"
"Red was let go, and he was not happy about it. We are worried that he might have done something to our network on the way out."
"OK, let me get some things ready, and I'll be over there shortly."
You knew this would be messy when you came in, but you did have some advantage in that you already knew the network. You had recommended many changes in the past, none of which would be implemented by Red. While pulling together your laptop and other tools, you grab your notes which have an overview of the network: Certkiller network notes: Single Internet access point, T1, connected to Certkiller Cisco router. Router has E1 to a private web and ftp server and E0 to the LAN switch. LAN switch has four servers, four printers, and100 client machines. All the machines are running Windows 2000. Currently, they are having their primary web site and email hosted by an ISP in Illinois.
When you get to Certkiller , the HR Director and the CEO, both of whom you already know, greet you. The CEO informs you that Red was let go due to difficult personality conflicts, among other

reasons, and the termination was not cordial.

You are to sign the proper employment papers, and get right on the job. You are given the rest of the day to get setup and running, but the company is quite concerned about the security of their network. Rightly so, you think, 'If these guys had implemented even half of my recommendations this would sure be easier.' You get your equipment setup in your new oversized office space, and get started. For the time you are working here, your IP Address is 10.10.50.23 with a mask of \16.

One of your first tasks is to examine the router's configuration. You console into the router, issue a show running-config command, and get the following output:

```
MegaOne#show running-config
Building configuration...
Current configuration:
!
version 12.1
service udp-small-servers
service tcp-small-servers
!
hostname MegaOne
!
enable secret 5 $1$7BSK3$H394yewhJ45JAFEWU73747.
enable password clever
!
no ip name-server
no ip domain-lookup
ip routing
!
interface Ethernet0
no shutdown
ip address 2.3.57.50 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
no shutdown
ip 10.10.40.101 255.255.0.0
no ip directed-broadcast
!
interface Serial0
no shutdown
ip 1.20.30.23 255.255.255.0
no ip directed-broadcast
clockrate 1024000
bandwidth 1024
encapsulation hdlc
```

```
!
ip route 0.0.0.0 0.0.0.0 1.20.30.45
!
line console 0
exec-timeout 0 0
transport input all
line vty 0 4
password remote
login
!
end
```

After analysis of the network, you recommend that the router have a new configuration. Your goal is to make the router become part of your layered defense, and to be a system configured to help secure the network.

You talk to the CEO to get an idea of what the goals of the router should be in the new configuration. All your conversations are to go through the CEO; this is whom you also are to report to.

"OK, I suggest that the employees be strictly restricted to only the services that they must access on the Internet." You begin.

"I can understand that, but we have always had an open policy. I like the employees to feel comfortable, and not feel like we are watching over them all the time. Please leave the connection open so they can get to whatever they need to get to. We can always reevaluate this in an ongoing basis."

"OK, if you insist, but for the record I am opposed to that policy." "Noted," responds the CEO, somewhat bluntly.

"All right, let's see, the private web and ftp server have to be accessed by the Internet, restricted to the accounts on the server. We will continue to use the Illinois ISP to host our main web site and to host our email. What else, is there anything else that needs to be accessed from the Internet?"

"No, I think that's it. We have a pretty simple network, we do everything in house." "All right, we need to get a plan in place as well right away for a security policy. Can we set something up for tomorrow?" you ask.

"Let me see, I'll get back to you later." With that the CEO leaves and you get to work.

Based on the information you have from Certkiller ; knowing that the router must be an integral part of the security of the organization, select the best solution to the organization's router problem:}

A. You backup the current router config to a temp location on your laptop. Friday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#no cdp run
MegaOne(config)#no ip source-route
MegaOne(config)#no ip finger
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 deny ip 0.0.0.0 255.255.255.255 any
MegaOne(config)#access-list 175 deny ip 10.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 127.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 deny ip 192.168.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface serial 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no ip directed broadcast
MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z
MegaOne#
```

B. You backup the current router config to a temp location on your laptop. Sunday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Ethernet 0
MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable
MegaOne(config)#interface Ethernet 1
MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable
MegaOne(config-if)#Z
MegaOne#
```

C. You backup the current router config to a temp location on your laptop. Early Monday morning, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Serial 0
MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable
MegaOne(config-if)#no ip directed broadcast MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z
MegaOne#
```

D. As soon as the office closes Friday, you get to work on the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Ethernet 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config)#interface Ethernet 1
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#Z
MegaOne#
```

E. With the office closed, you decide to build the new router configuration on Saturday. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#no cdp run
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 deny ip 0.0.0.0 255.255.255.255 any
MegaOne(config)#access-list 175 deny ip 10.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 127.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 deny ip 192.168.0.0 0.0.255.255 any
MegaOne(config)#no ip source-route
MegaOne(config)#no ip finger
MegaOne(config)#interface serial 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no ip directed broadcast
MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z
MegaOne#
```

Answer: B

- QUESTION NO : 4

It has been quite some time since you were called in to address the network and security needs of Certkiller . You feel good in what you have accomplished so far.

You have been able to get Certkiller to deal with their Security Policy issue, you have secured the router, added a firewall, added intrusion detection, hardened the Operating Systems, and more. One thing you have not done however is run active testing against the network from the outside. This next level of testing is the final step, you decide, in wrapping up this first stage of the new Certkiller network and security system. You setup a meeting with the CEO to discuss.

"We have only one significant issue left to deal with here at Certkiller ," you begin.

"We need some really solid testing of our network and our security systems."

"Sounds fine to me, don't you do that all the time anyway? I mean, why meet about this?"

"Well, in this case, I'd like to ask to bring in outside help. Folks who specialize in this sort of thing. I can do some of it, but it is not my specialty, and the outside look in will be better and more independent from an outside team."

"What does that kind of thing cost, how long will it take?"

"It will cost a bit of money, it won't be free, and with a network of our size, I think it can be done pretty quick. Once this is done and wrapped up, I will be resigning as the full time security and network pro here. I need to get back to my consulting company full time. Remember, this was not to be a permanent deal. I can help you with the interview, and this is the perfect time to wrap up that transition." All right, fair enough. Get me your initial project estimates, and then I can make a more complete decision. And, I'll get HR on hiring a new person right away."

Later that afternoon you talk to the CEO and determine a budget for the testing.

Once you get back to your office, you are calling different firms and consultants, and eventually you find a consulting group that you will work with.

A few days later you meet with the group in their office, and you describe what you are looking for, and that their contact and person to report to is you. They ask what is off limits, and your response is only that they cannot do anything illegal, to which they agree and point out is written in their agreement as well.

With this outside consulting group and your knowledge of the network and company, review and select the solution that will best provide for a complete test of the security of Certkiller .}

A. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.

The first thing the consultants will do is dumpster diving and physical surveillance, looking for clues as to user information and other secret data that should not be outside of the network. Once they have identified several targets through the dumpster diving, they will run scans to match up and identify the workstations for those users.

After identifying the user workstations, they will run vulnerability checks on the systems, to find holes, and if a hole is found they have been given permission to exploit the hole and gain access of the system.

They will attempt to gain access to the firewall and router remotely, via password guessing, and will test the response of the network to Denial of Service attacks. Finally, they will call into Certkiller to see what information they can learn via social engineering.

B. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.

The consultants will first run remote network surveillance to identify hosts, followed by port scans and both passive and active fingerprinting. They will then run vulnerability scanners on the identified systems, and attempt to exploit any found vulnerabilities. They will next scan and test the router and firewall, followed by testing of the IDS rules.

They will then perform physical surveillance and dumpster diving to learn additional information. This will be followed by password sniffing and cracking. Finally, they will call into Certkiller to see what information they can learn via social engineering.

C. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.

The consultants surprise you with their initial strategy. They intend to spend nearly 100% of their efforts over the first week on social engineering and other physical techniques, using little to no technology. They have gained access to the building as a maintenance crew, and will be coming into the office every night when employees are wrapping up for the day.

All of their testing will be done through physical contact and informal questioning of the employees. Once they finish that stage, they will run short and direct vulnerability scanners on the systems that they feel will present weakness.

D. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.

The consultants have decided on a direct strategy. They will work inside the Certkiller office, with the group introducing themselves to the employees. They will directly interview each employee, and perform extensive physical security checks of the network.

They will review and provide analysis on the security policy, and follow that with electronic testing. They will run a single very robust vulnerability scanner on every single client and server in the network, and document the findings of the scan.

E. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.

The consultants will start the process with remote network surveillance, checking to see what systems and services are available remotely. They will run both passive and active fingerprinting on any identified system. They will run customized vulnerability scanners on the identified systems, and follow that through with exploits, including new zero-day exploits they have written themselves.

They will next run scans on the router, firewall, and intrusion detection, looking to identify operating systems and configurations of these devices. Once identified, they will run customized scripts to gain access to these devices. Once they complete the testing on the systems, they will dumpster dive to identify any leaked information.

Answer: C

- QUESTION NO : 5

Certkiller is a company that makes state of the art aircraft for commercial and government use.
Recently Certkiller has been working on the next generation of low
orbit space vehicles, again for both commercial and governmental markets.

Certkiller has corporate headquarters in Testbed, Nevada, USA. Testbed is a small town, with a population of less than 50,000 people. Certkiller is the largest company in town, where most families have at least one family member working there.

The corporate office in Testbed has 4,000 total employees, on a 40-acre campus environment. The largest buildings are the manufacturing plants, which are right next to the Research and Development labs. The manufacturing plants employee approximately 1,000 people and the R&D

labs employ 500 people. There is one executive building, where approximately 500 people work. The rest of the employees work in Marketing, Accounting, Press and Investor Relations, and so on. The entire complex has a vast underground complex of tunnels that connect each building. All critical functions are run from the Testbed office, with remote offices around the world. The remote offices are involved in marketing and sales of Certkiller products.

These offices also perform maintenance on the Certkiller aircraft and will occasionally perform R&D and on-site manufacturing.

There are 5 remote offices, located in: New York, California, Japan, India, and England. Each of the remote offices has a dedicated T3 line to the Certkiller HQ, and all network traffic is routed through the Testbed office - the remote offices do not have direct Internet connections.

You had been working for two years in the New York office, and have been interviewing for the lead security architect position in Testbed. The lead security architect reports directly to the Chief Security Officer (CSO), who calls you to let you know that you got the job. You are to report to Testbed in one month, just in time for the annual meeting, and in the meantime you review the overview of the Certkiller network.

Your first day in Certkiller Testbed, you get your office setup, move your things in place, and about the time you turn on your laptop, there is a knock on your door. It is Blue, the Chief Security Officer, who informs you that there is a meeting that you need to attend in a half an hour.

With your laptop in hand, you come to the meeting, and are introduced to everyone. Blue begins the meeting with a discussion on the current state of security in
Certkiller .

"For several years now, we have constantly been spending more and more money on our network defense, and I feel confident that we are currently well defended." Blue, puts a picture on the wall projecting the image of the network, and then continues, "We have firewalls at each critical point, we have separate Internet access for our public systems, and all traffic is routed through our controlled access points. So, with all this, you might be wondering why I have concern."

At this point a few people seem to nod in agreement. For years, Certkiller has been at the forefront of perimeter defense and security. Most in the meeting are not aware that there is much else that could be done.

Blue continues, "Some of you know this, for the rest it is new news: MassiveCorp is moving their offices to the town right next to us here. Now, as you all know,
MassiveCorp has been trying to build their orbital systems up to our standards for years and have never been able to do so. So, from a security point of view, I am concerned."

This is news to most people, Green, the Vice President of Research asks, "We have the best in firewalls, we have the best in you and your systems, what are you suggesting?"

Blue responds, "I suggest trust. Not with MassiveCorp, but in our own systems. We must build trusted networks. We must migrate our network from one that is well-defended to one that is welldefended
and one that allows us to trust all the network traffic."

The meeting continues for some time, with Blue leading the discussion on a whole new set of technologies currently not used in the network. After some time, it is agreed upon that Certkiller will migrate to a trusted networking environment.

The following week, Blue informs you that you will be working directly together on the development of the planning and design of the trusted network. The network is going to run a full PKI, with all clients and servers in the network using digital certificates. You are grateful that in the past two years, Blue has had all the systems changed to be running only Windows 2000, both server and professional systems, running Active Directory. You think the consistent platform will make the PKI roll out easier.

The entire Certkiller network is running Active Directory, with the domain structure as in the following list:

Testbed. Certkiller .org
Newyork. Certkiller .org
California. Certkiller .org
Japan. Certkiller .org
India. Certkiller .org
England. Certkiller .org

Although you will be working in the Testbed office, the plan you develop will need to include the entire Certkiller organization.

Based on this information, select the solution that describes the best plan for the new trusted network of Certkiller :}

A. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a CPF based on your own guidelines, including physical and technology controls.
3. Design the system to be a full hierarchy, with the Root CA located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.
4. Design the hierarchy with each remote office and building having it's own enrollment CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
7. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.

B. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with

their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.

2. Draft a CPF based on your own guidelines, including physical and technology controls.

3. Design the system, outside of the executive office, to be a full hierarchy, with the Root CA for the hierarchy located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.

4. In the executive building, you design the system to be a mesh CA structure, with one CA per floor of the building.

5. Design the hierarchy with each remote office and building having it's own enrollment CA.

6. Build a small test pilot program, to test the hierarchy, and integration with the existing network.

7. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.

8. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.

9. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.

10. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.

11. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.

C. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

1. Draft a Certificate Policy (CP) document to define what users will be allowed to do with their certificates, and a Certification Practice Statement (CPS) document to define the technology used to ensure the users are able to use their certificates as per the CPS.

2. Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component.

3. Design the system to be a full hierarchy, with the Root CA located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.

4. Design the hierarchy with each remote office and building having it's own enrollment CA.

5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.

6. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.

7. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.

8. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.

9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.

10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.

D. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

1. Draft a Certificate Policy (CP) document to define what users will be allowed to do with their certificates, and a Certification Practice Statement (CPS) document to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component.
3. Design the system to be a full mesh, with the Root CA located in the executive building.
4. Design the mesh with each remote office and building having it's own Root CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA mesh in the executive office, and get all users acclimated to the system.
7. Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.

E. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a CPF based on your own guidelines, including physical and technology controls.
3. Design the system to be a full mesh, with the Root CA located in the executive building.
4. Design the mesh with each remote office and building having it's own Root CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA mesh in the executive office, and get all users acclimated to the system.
7. Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.

Answer: E