Free Questions for SC0-502 by ebraindumps

Shared by Ortiz on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

By now, you are feeling confident that the security of the MegaCorp network is getting under control. You are aware that there are still several critical areas that you must dealwith, and today you are addressing one of those areas. You have been able to take care of the router, firewall, security policy, and intrusion detection, now you are concerned with some of the hosts in the network. Since the organization is not very large, you are the only person working in the IT end of the company. Itwill be up to you to directly work on the systems throughout the network. You make a quick chart of the systems you know should be in the MegaCorp network:

Server0001, 10.10.20.101, Windows 2000 Server Server0010, 10.10.20.102, Windows 2000 Server Server0011, 10.10.20.103, Windows 2000 Server Server0100, 10.10.20.104, Linux (Red Hat 8.0) User systems, 10.10.100.100~10.10.100.200, Windows 2000 Professional The addressing that you recommended months ago is in place, and it follows a distinct logical pattern,you are hoping that no new systems are hidden in the network somewhere. In the company, you have been granted domain administrator rights, and no other user is authorized tohave administrator, root, supervisor, or otherwise privileged level of access. All the Windows systems are to belong to one windows domain called SCNA.edu. Users are no longer allowed to install unauthorized applications, and are all to use the file servers for storage. Although they have the ability to do so, users are not supposed to store any work data on their local systems. The servers are located in a server cabinet that is inside your office, so you decide to start working there. Using your knowledge of MegaCorp select the best solution for hardening the MegaCorp operating systems:}

Options:

A- The first thing you do is to run a Nessus scan against all the servers in the room, noting the findings of the scans. You then begin on the servers by running some tests on the Linux server. First, you run Tripwire on the entire system to ensure that there are no rogue

Root accounts, and the test is positive. Second, you ensure that there are no unauthorized objectsavailable through the network, and third you lock the system down with Bastille. You then work on the Windows servers. You run a check to ensure there are no unauthorized administrator accounts, and there are not. You create a custom security template and implement the template on each server using the Security Configuration and Analysis Snap-In, and you ensure that each system is updated with the latest patches. Finally, you analyze the user desktops. You go one by one through the network checking for added user accounts, and you find some. You remove these unauthorized accounts and check for software and applications. Again, you find some applications that are not allowed and you remove them.You check the systems for hardware changes, and address the issues that you find.

B- You start the job by running some analysis on the Windows servers. You do this using the Security Configuration and Analysis Snap-In, and you ensure that each system is updated with the latest patches. You find several user accounts that have been given local administrator access, and youremove these accounts. You next use the Secedit tool to implement local encryption on the shared hard drive to secure the local files for the network users.You then work on the Linux server. To your surprise there are nounauthorized root accounts, nor any unauthorized shares. You ensure that the permissions are correct on the shared objects, and run Bastille to lock down the server. You then work on the client machines. Before you physically sit at each machine, you run a Nessus scan from your office. Bringing the results with you, you go to each machine andaddress any issues as identified in the Nessus scan, remove any unauthorized applications

C- The first thing you decide to do is plug your laptop into the server room, and run a full Nessus scan on the entire network, specifically looking for every backdoor vulnerability that theapplication can check. This takes some time to compile, but you eventually end up with a list of issues to address on each machine. You move on to the Linux server, and run a fast Tripwire check on the system to look forany additional vulnerabilities. Once that check is done, you install SSH so that all access by every user will be encrypted to the server, and you run Bastille to lock down the system. At the Windows systems, you address any issues found during the Nessus scan, you ensure that each system is updated with the latest patches, and you ensure that the systems are allfunctioning as fully secure and functional file servers to the network by implementing the HISECWEB.INFtemplate in the Security Configuration and Analysis Snap-In.Finally, you work on each desktop machine by removing any vulnerabilities listed in the scan report. You remove a few pieces of unauthorized hardware and many unauthorized applications.

D- You being by running a Nessus scan from your office laptop on the systems in the network, first the servers, then the user workstations. After the scans are complete, you store the reports on your laptop, and you take your laptop to the server room. In the server room, you begin on the Windows servers. You implement a custom security template on eachserver using the Security Configuration and Analysis Snap-In, remove any unauthorized accounts, ensure that each system is updated with the latest patches, and ensure that the permissions on each shared object are as per policy. You then work on the Linux server, by addressing each point identified in the Nessusscan. You then lock thesystem with Bastille, ensure that each system is updated with the latestpatches, and run a quick Tripwire scan to create a baseline for the system. You take your laptop with you as you go throughout the network to each userworkstation, ensure that each system is updated with the latest patches, and you take care of each issue you found on the machines. There are a few systems that you find with unauthorized applications and you removethose applications.

E- You begin by running a Nessus scan on each computer in the network, using the \hotfix switch to create a full report. The report identifies every vulnerability on each system and lists the specific changes you must make to each system to fix any found vulnerabilities. You take the report to the server room and start with the Linux server. On the server, you run through the steps as outlined in the Nessus report, and end by locking the system using Bastille. Then, you move to the Windows systems, again following the steps of the Nessus report, and ending by using the Security Configuration and Analysis Snap-In to implement the GoldStandard template on every server. Finally, you proceed to each user workstation. At each user machine, you follow each step for each system, based on your report. Once you have addressed all the vulnerabilities in the systems, you run a quick Secedit scan on each system to ensure that they are all locked down and that proper encryption is configured.

Answer:

D

Question 2

Question Type: MultipleChoice

Things have been running smoothly now at GlobalCorp for the last several weeks. There have been no major attacks, and it seems that the systems in place are performing just as expected. You are putting together some paperwork when you get a call from Orange to meet in the conference room. When you get there, Orange is wrapping up a meeting with the senior Vice President of Sales, whom you say hello to on your way in. "I was just talking with our senior VP here, and we're run into a new issue to discuss," Orange tells you. "Wel Il let you two sort this out. Orange, do let me know when it all ready to go."With that the VPleaves. You sit down across from Orange, who starts, "That was an interesting meeting. It seems that even though I have always said no to the request, we are being pressured to implement a wireless network." "Here?" you ask, "In the executive building?""Yes, right here. The sales team wishes to have the ability to be mobile. Instead of running a full scale roll out I have trimmed the request down to running a test implementation on the second floor. The test run on that floor will be used to determine the type of wireless rollout for the rest of the building, and eventually the rest of the campus. So, here is what we need to do. I need you to create the roll out plan, and bring that plan to me. Il review with you and implement as required." "As always, what is my budget restriction?" you ask. "In this case, security is the top priority. If we are going to run wireless, it has to be as secure as possible, use whatever you need. That being said, your plan has to use existing technologies, we are not going to fund the development of a new protocol or proprietary encryption system right now."You begin your work on this problem by pulling out your own wireless networking gear. You have alaptop that uses an ORiNOCO card, and you have a full directional antenna that you can holdor mount on a small tripod. You take your gear to the lobby of the second floor, and you load up Net Stumbler quickly to run a quick check that there are no access points in your area. The immediate area is clear of any signal, so you take you gear and walk the entiresecond floor, waitingto see if there is any signal, and you find none. With your quick walk through complete, you take your gear back to your office and start working on your plan. Using your knowledge of the GlobalCorp network, select the best solution to the wireless networking rollout problem:}

Options:

A- You have figured out that since the network is a test roll out, you have some flexibility in its configuration. After your walk through test, you begin by configuring the wireless nodes in the network to run in Ad Hoc mode, creating an Independent Basic Service Set (IBSS). You will use a complex SSID of 5cN@4M3! on all wireless nodes. You will next configure every node to nolonger broadcast any beacon packets. You will configure all the nodes to not use the default channel, and instead move them all to channel six. You will configure every node to use MAC address filtering, to avoid unauthorized nodes from attempting to gain access to the network. Finally, you will configure each node to use WEP in the strong 128-bit mode, along with a complex 16-character passphrase. Once the network is up and running, you take your gear (which is not an authorized client of the network) and every few days will walk the office again, checking for access. B. You have figured out that since the network is a test roll out, you have some flexibility in its configuration. After your walk through test, you begin by configuring the wireless nodes in the network to run in Ad Hoc mode, creating an Extended Basic Service Set (EBSS). You will use a complex SSID of 5cN@4M3! on all wireless nodes. You will next configure every node to no longer broadcast any beacon packets. You will configure all the nodes to not use the default channel, and instead move them all to channel six.You will configure every node to use MAC address filtering, to avoid unauthorized nodes from attempting to gain access to the network. Finally, you will configure each node to use WEP inthe strong 128-bit mode, along with a complex 16-character passphrase for generating four keys. You willmanually input the WEP Keys into each node. You will divide the test nodes into quarters, and configure each quarter to startup on the network using a different default WEP key. Once the network is up and running, you take your gear (which is not an authorized client of the network) and every few days will walk the office again, checking for access.

C- You determine that for the test network, you will run the network in infrastructure mode, using a SSID ofFLOOR2. During the test, you will create one single Basic Service Set (BSS),running through one access point. All test nodes will be configured to participate in theBSS, using the SSID ofFLOOR2, and the access point will be configured with MAC address filteringof the test nodes. You will configure the access point to use EAP, specifically EAP-TLS. You willconfigure a Microsoft RADIUS Server as the authentication server. You will configure the RADIUS server with a digital certificate. Using EAP-TLS, both the server and the client will be required to authenticate using their digital certificates before full network access will be granted. Clients will have supplicant software configured where required. You will next make a physical map of the office, using the tool Ekahau. Working with this tool, you will map out and track the positioning of each wireless device once the network isactive. When the network is up and running, you take your gear (which is not an authorized client of the network) and every few days will walk the office again, checking for access. You will continue the test by

running checks from the parking lot, ensuring that you cannot gain access.

D- You determine that for the test network, you will run in infrastructure mode, using a SSID of FLOOR2. During the test, you will create one single Independent Basic Service Set (IBSS), running through one access point. All test nodes will be configured to participate in the IBSS, using the SSID of FLOOR2. You will configure the access point to use WPA, with an algorithm of TKIP. You will configure WPA to utilizethe full 128-bit key option, with the pre-shared WPA key option. The clientcomputers will need supplicants, so you will configure the Funk Software Odyssey Client on the clients, matching the key settings and TKIP settings.You will disable the access point from broadcasting its SSID, and you will configureMAC address filtering. Once the network is up and running, you take your gear (which is not an authorized client of the network) andevery few days will walk the office again, checking for access.

E- You figure out that you will run the test network in infrastructure mode, using a SSID of GlobalCorp. You will create one single Basic Service Set (BSS), all running through one accesspoint. All test nodes will be configured to participate in the BSS, using the SSID of GlobalCorp, and the accesspoint will be configured with MAC address filtering of the test nodes.You will configure the access point to utilize a combination of 802.1x and WPA. The WPA settings will befully secured with TKIP, and 128-bit keys, which change on a per session basis. The 802.1x settings will be to use Lightweight EAP (LEAP). The clients will be configured to use LEAP, witha fallback to TKIP at 128-bits.You will configure the access point to utilize a combination of 802.1x and WPA. The WPA settings will be fully secured with TKIP, and 128-bit keys, which change on a per session basis. The 802.1x settings will be to use Lightweight EAP (LEAP). The clients will be configured to use LEAP, with a fallback to TKIP at 128-bits. When the network is up and running, you take your gear (which is not an authorized client of the network) and every few days will walk the office again, checking for access. You will continue the test by running checks from the parking lot, ensuring that you cannot gain access.

Answer:

C

Question 3

Question Type: MultipleChoice

The network has been receiving quite a lot of inbound traffic, and although you have been given instructions to keep the network open, you want to know what is going on. You havedecided to implement an Intrusion Detection System. You bring this up at the next meeting. "After looking at our current network security, and the network traffic we are dealing with, I recommend that we implement an Intrusion Detection System," you begin. "We don't have any more budget for security equipment, it will have to wait until next year." This is the reply from the CEO that you were anticipating. "I realize that the budget is tight, but this is an important part of setting up security." You continue, "If Icannot properly identify all the network traffic, and have a system in place to respond to it, we might not know about an incident until after our information is found for sale on the open market."As expected, your last comment got the group thinking. What about false alarms?" asks the VP of sales, "I hear those things are always goingoff, and just endup wasting everyone" time.""Tha's a fair concern, but it is my concern. When we mplement the system, I will fine tune it and adjust t until the alarms it generates are ppropriate, and are generated when there is egitimately something to be concerned about.We are concerned with traffic that would indicate anattack; only then will the ystem send me an alert." or a few minutes there was talk back and forth in the room, and hen the CEO responds again to your nquiry, "I agree that this type of thing could be helpful. But, we simply don have any morebudget for it. Since it is a good idea, go aheadand find a way to implement this, but don't spend any oney on it."With this nformation, and your knowledge of MegaCorp, choose the answer that will provide the bestsolution for the IDS needs of MegaCorp:}

Options:

A- You install Snort on a dedicated machine just outside the router. The machine is designed to send alerts toyou when appropriate. You implement the following rule set: Alert udp any any -> 10.10.0.0\16 (msg: 'O\S Fingerprint Detected'; flags: S12;)Alert tcp any any -> 10.10.0.0\16 (msg: 'Syn\Fin Scan Detected'; flags: SF;)Alert tcp any any -> 10.10.0.0\16 (msg: 'Null Scan Detected'; flags: 0;) og tcp any

any -> 10.10.0.0\16 any You then install Snort on the web and ftp server, also with this system designed to send ou alerts whenappropriate. You implement the built-in scan.rules ruleset on the server.

B- You configure a new dedicated machine just outside the router and install Snort on thatmachine. Themachine logs all intrusions locally, and you will connect to the machine remotelyonce each morning to pull the log files to your local machine for analysis. ou run snort with the following command: Snort ev \snort\log snort.conf and using the following ule base: lert tcp any any <> any 80 lert tcp any any <> 10.10.0.0\16 any (content: 'Password'; msg:'Password transfer Possible';) Log tcp any any <- 10.10.0.0\16 23 Log tcp any any <> 10.10.0.0\16 1:1024

C- You install your IDS on a dedicated machine just inside the router. The machine is designed to send alerts o you when appropriate. You begin the install by performing a new install of indows on a clean hard drive. ou install ISS Internet Scanner and ISS System Scanner on the new system. System canner is configured todo full backdoor testing, full baseline testing, and full password testing.Internet Scanner is configured with a custom policy you made to scan for all vulnerabilities. You configure both canners to generate automatic weekly reports and to send you alerts whenan incident of note takes place on the network.

D- You install Snort on a dedicated machine just inside the router. The machine is designed to send alerts to ou when appropriate. You do have some concern that the system will have toomany rules to operate efficiently. To address this, you decide to pull the critical rules out of the built-in rule ets, and create one simple rule set that is short and will cover all of the seriousincidents that the network might experience. alert udp any 19 <>
$HOME_NET 7 (msg:'DOS UDP Bomb'; classtype:attempted-dos;sid:271; rev:1;) lert udp $EXTERNAL_NET any
-> $HOME_NET any (msg:'DOS Teardrop attack';id:242; fragbits:M;classtype:attempted-dos; sid:270;
rev:1;)alert icmp
$EXTERNAL_NET any -> $HOME_NET any (msg:'DDOS TFN Probe'; id: 678; itype: 8;
content:'1234';classtype:attempted-recon; sid:221; rev:1;) lert icmp XTERNAL_NET any ->
$HOME_NET any (msg:'ICMP PING NMAP'; size:;itype:8;classtype:attempted econ; sid:469;
rev:1;)alert tcp $EXTERNAL_NET any -> $HOME_NET any msg:'SCAN
XMAS';flags:SRAFPU; lasstype:attempted-recon; sid:625; rev:1;) lert tcp HOME_NET 31337
> $EXTERNAL_NET 80 (msg:'SCAN synscan microsoft'; id: 9426; flags: F;

lasstype:attempted-recon; sid:633; rev:1;)

E- You install two computers to run your IDS. One will be a dedicated machine that is on the outside of therouter, and the second will be on the inside of the router. You configure themachine on the outside of the router to run Snort, and you combine the default rules of several of the built-inrule sets. You combine the ddos.rules, dos.rules, exploit.rules, icmp.rules, nd scan.rules. n the system that is inside the router, running Snort, you also combine several of thebuilt-in rule sets. You combine thes can.rules,webcgi.rules,ftp.rules, web-misc.rules, andweb-iis.rules.You configure the alerts on the two systems to send youemail messages when events are identified. After youimplement he two systems, you run some external scans and tests using vulner ability checkers and exploit testing software. You modify your rules based on your tests.

Answer:

E

Question 4

Question Type: **MultipleChoice**

You had been taking a short vacation, and when you come into work on Monday morning, Orange is already at your door, waiting to talk to you. "We're got a problem," Orange says, "It seems that the password used by our Vice President of Engineering has been compromised. Over the weekend, we found this account had logged into the network 25 times. The Vice President was not even in the office over the weekend." "Did we get the source of the compromise yet?" "No, but it won't surprise me if it is our new neighbors at MassiveCorp. I need to you to come up with a realistic plan and bring it to me tomorrow afternoon. This problem must be resolved, and like everything else we do not have unlimited funds so keep that in mind." Based on this information, choose the best solution to the

password local authentication problem in the Executive building.}

Options:

A- Since you are aware of the significance of the password problems, and since you do not have unlimited funds, you plan to address this problem through education and through awareness. You write up a plan for Orange that includes the following points:
1.All end users are to be trained on the methods of making strong passwords
2.All end users are instructed that they are to change their password at a minimum of every 30 days. 3.The administrative staff is to run password-checking utilities on all passwords every 30 days.
4.All end users are to be trained on the importance of never disclosing their password to any other individual.
5.All end users are to be trained on the importance of never writing down their passwords where they areclearly visible.

B- Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Orange that includes the following points: 1.You will reconfigure the Testbed.globalcorp.org domain to control the password problem. 2.You will configure AD in this domain so that complex password policies are required. 3.The complex password policies will include: a.Password length of at least 8 characters b.Passwords must be alphanumeric c.Passwords must meet Gold Standard of complexity d.Passwords must be changed every 30 days e.Passwords cannot be reused

C- Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Orange that includes the following points:
1.For all executives you recommend no longer using passwords, and instead migrating to a token-based authentication system.
2.You will install the RSA SecurID challenge-response token system.
3.You will create SecurID user records for each user to match their domain accounts.
4.You will assign each user record a unique token.

5.You will hand deliver the tokens to the correct executive.
6.Users will be required to use tokencodes from the One-Time tokencode list. The tokencodes will be alphanumeric and will be 4 characters long.
7.The tokens will replace all passwords for authentication into each user Windows system.

D- Since you are aware of the significance of the password problems, plan to address the problem using technology. You write up a plan for Orange that includes the following points:
1.For all executives you recommend no longer using passwords, and instead migrating to a biometric solution.
2.You will install retinal scanners at every user desktop in the executive building.You will install retinal scanners at every user? desktop in the executive building.
2.You will install retinal scanners at every user desktop in the executive building.You will install retinal scanners at every user? Desktop in the executive building.
3.You will personally enroll each user at each desktop.3.You will personally enroll each user at each desktop.
4.You will instruct each user on the proper positioning and use of the scanner.4.You will instruct each user on the proper positioning and use of the scanner. 5.The biometric system will replace all passwords for authentication into each user Windows system.The biometric system will replace all passwords for authentication into each user?
Windows system. 6.The biometric system will replace all passwords for authentication into each user Windows system.The biometric system will replace all passwords for authentication into each user? Windows system.

E- Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Orange that includes the following points:
1.For all executives you recommend no longer using passwords, and instead migrating to a token-based authentication system.
2.You will install the RSA SecurID time-based token system. 3.You will create SecurID user records for each user to match their domain accounts. 4.You will assign each user record a unique token. 5.You will hand deliver the tokens to the correct executive. 6.Users will be allowed to create their own PIN, which will be 4 characters long.
7.The tokens will replace all passwords for authentication into each user Windows system.

Answer:

E

Question 5

Question Type: MultipleChoice

You have now seen to it that all end users and computers in the Testbed office have received their certificates. The administrative staff has been trained on their use and function in the network. The following day, you meet with Orange to discuss the progress. "So far so good," starts Orange, "all the users have their certificates, all the computers have their certificates. I think we are moving forward at a solid pace. We have talked about the ways we will use our certificates, and we need to move towards securing our network traffic." "I agree," you reply, "last week I ran a scheduled scan, and we still have vulnerability in our network traffic. The folks from MassiveCorp would love to have a sniffer running in here, I sure of that." "That exactly the point. We need a system in place that will ensure that our network traffic is not so vulnerable to sniffing. We have to get some protection for our packets. I like you to design the system and then we can review it together." The meeting ends a few minutes later, and you are back in your office working on the design. Choose the best solution for protecting the network traffic in the executive office of the Testbed campus:}

Options:

A- After further analysis on the situation, you decide that you will need to block traffic in a more completeway at the border firewalls. You have decided that by implementing stricter border control, you will be able to manage the security risk of the packets that enter and leave the network better. You implement a new firewall at each border crossing point. You will configure half of the firewalls with Checkpoint

FW-1 NG and the other half with Microsoft ISA. By using two different firewalls, you are confident that you will be minimizing any mass vulnerability. At each firewall you implement a new digital certificate for server authentication, and you configure thefirewall to require every user to authenticate all user connections. You block all unauthorized traffic and run remote test scans to ensure that no information is leaking through. Once the test scans are complete, you verify that all users are required to authenticate with the new firewall before their traffic is allowed to pass, and everything works as you planned.

B- You spend time analyzing the network and decide that the best solution is to take advantage of VPN technology. You will create one VPN endpoint in each building. Your plan is to create aunique tunnel between each building.You first install a new Microsoft machine, and configure it to perform the functions ofRouting and RemoteAccess. You then create a tunnel endpoint, and configure each machine to use L2TP to create the tunnel. To increase security, you will implement full 256-bit encryption on each tunnel, and you will use 3DES on onehalf of the tunnels and AES on the other half of the tunnels. You will be sure that each tunnel uses the same algorithm on both ends, but by using two algorithms you are sure that you haveincreased the security of the network in a significant way.

C- You decide that you will implement an IPSec solution, using custom IPSec settings. You wish to utilize thedigital certificates that are available in the network. You decide that you wish for there to be maximum strength, and therefore you choose to implement IPSec using both AH and ESP. First, you configure a custom policy for the servers in the network. You verify that none of the default policies are currently implemented, and you create a new policy. Your new policy will use SHA for AH and SHA+3DES for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the servers that you can and use secedit to force the others to refresh their policy. Next, with the help of the administrative staff, you will configure each client in the network. For the clients, you verify that no default policy is enabled, and you create a policy that uses SHA for AH and SHA+3DES for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the client machines that you can and use secedit to force the others torefresh their policy.

D- You decide that you will implement an IPSec solution, using the built-in functionality of Windows. You decide that you wish for there to be maximum strength, and therefore you choose toimplement IPSec using both AH and ESP. First, you configure each server in the network with a new IPSec policy. You choose to implement the defaultServer IPSec Policy. Using this policy you are sure that all communication both to and from the server will utilize IPSec. You reboot the servers that you can and usesecedit to

force the others to refresh their policy. Next, with the help of the administrative staff, you will configure each client in the network. For the clients, you use the default Client IPSec Policy. You reboot the client machines that you can and use secedit to force the others to refresh their policy.

E- You decide that you will implement an IPSec solution, using custom IPSec settings. You wish to utilize the digital certificates that are available in the network. You decide that you wish for there to be maximum strength, and therefore you choose to implement IPSec using both AH and ESP. First, you configure a custom policy for the servers in the network. To increase strength, you will implement your custom policy on top of the default Server IPSec Policy. You verify that the policy is running, and then you create a new policy. Your new policy will use SHA+3DES for AH and SHA for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the servers that youcan and use secedit to force the others to refresh the two policies. Next, with the help of the administrative staff, you will configure each client in the network. For the clients you also need the highest in security, so you will use a custom policy on the default policy. You verify that the default Client IPSec policy is enabled, and then you create a policy that uses SHA+3DES for AH and SHA for ESP. You make sure that the policy is toinclude all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the client machines that you can and use secedit to force the others to refresh the two policies.

Answer:

C

Question 6

Question Type: MultipleChoice

You have now been involved in several major changes in the security of GlobalCorp, and specifically the Testbed campus. You have worked on the planning and design of the trusted network, you have worked on the initial rollout of the CA hierarchy, you have worked on assigning certificates to the end users and computers in the Executive building of the Testbed campus, and you have managed the implementation of secure email a critical service for GlobalCorp. Blue has asked you to meet with the other administrative staff of the Testbed campus and discuss how the certificates will impact the organization. There are a total of about 40 people in the meeting, and you have decided that your primary focus during this meeting will be on encryption\cryptography. Choose the best solution for providing the correct information to your administrative staff on how encryption\cryptography and digital certificates will be properly used in the network:}

Options:

A- You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the GlobalCorp network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA has a pair of keys and UserB has a pair of keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB. 'We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the public key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, called the private key, to decrypt the message,' you explain to the group. You further explain some of the common algorithms used in the network. You tell them that Diffie-Hellman was the first widely used public key algorithm, and that Diffie-Hellman itself is not used to secure messages, rather to exchange a symmetric key. You explain that RSA was another breakthrough in that it was a public key algorithm that was able to secure messages. You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished

name of the person who has the private key that corresponds to the public key in the certificate.

B- You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the GlobalCorp network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA has a pair of keys and UserB has a pair of keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB. 'We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserB will use the public key that UserA has made available to encrypt the message. Once encrypted, UserB will send the message over the network to UserA. UserA will then use the other key of the pair, the private key to decrypt the message,' you explain to the group. You further explain some of the common algorithms used in the network. You tell them that Diffie-Hellman was the first widely used private key algorithm, and that Diffie-Hellman itself is not used to secure messages, rather to exchange a symmetric key. You explain that RSA was another Break through in that it was a private key algorithm that was able to secure messages. You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.

C- You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the GlobalCorp network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA and UserB have a set of mathematically linked keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB. 'We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the public key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the private key to decrypt the message,' you explain to the group. You further explain some of the common algorithms used in the network. You tell them that RSA was the first widely used private key algorithm, and that RSA itself is not used to secure messages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough in that it was a private key algorithm that was able

to secure messages. You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.

D- You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the GlobalCorp network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA and UserB have a set of mathematically linked keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB. 'We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the private key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the public key to decrypt the message,' you explain to thegroup. You further explain some of the common algorithms used in the network. You tell them that RSA was the firstwidely used private key algorithm, and that RSA itself is not used to securemessages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough in that it was a private key algorithm that was able to secure messages. You then describe digital certificates and some of their features. You tell the group that digital certificates can beassigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holdsthe distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.

E- You gather the administrative staff together in the conference room to discuss cryptography in the network.You begin your talk with the function of cryptography, in general, and then youmove towards specific implementations in the GlobalCorp network.You explain that public key cryptography is founded on math, and that the big picturefundamental point is thatUserA and UserB have a set of mathematically linked keys. You explain that one key ofeach key pair is made available to the other users in the network. You illustrate this with an exampleof sending an encrypted message from UserA to UserB. 'We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the private key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the

public key to decrypt the message,' you explain to thegroup.You further explain some of the common algorithms used in the network. You tell them that RSA was the first widely used private key algorithm, and that RSA itself is not used to securemessages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough inthat it was a private key algorithm that was able to secure messages. You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds thedistinguishedname of the person who issued the certificate, and a Subject Field that holds thefull OIDs describing the use of the certificate by the holder of the certificate.

Answer:

A

Question 7

Question Type: **MultipleChoice**

Now that the network is moving towards a trusted network, you are preparing for the specific new implementations in GlobalCorp. Just as you wrap up some paperwork for the morning, Orange calls you and lets you know that you are going to be needed in a meeting this afternoon. You get to Orange's office and sit down at the desk. Orange begins the conversation, " You know we have some solid fundamental issues addressed in our new trusted network, but I have yet to feel that we have addressed any serious concerns." "Ie been thinking about some similar issues," you reply. "Good, then I sure you have been thinking about our email. Right now, I cannot guarantee the integrity of any email, and I cannot guarantee the confidentiality of any email. We have reasonable controls towards guaranteeing the availability of our email, but what the point if there is no confidentiality or integrity?" "I agree. I think that addressing this

issue should be an immediate priority." "One concern is that whatever the system is that we put in place, it must be very user-friendly. As we roll out these new systems, anything that will significantly increase the calls into the help desk is something we need to minimize. A second concern is that it not be too costly. We already have this new investment in the trusted network, we need to be sure that we utilize what are building to the fullest extent possible." "I think we should be able to do that without much difficulty. I already have some solid ideas," you reply. "OK, take a few days on this. For the moment, just concern yourself with the executive building; the others can follow the plan in their own buildings. Let meet again this coming Monday and you can describe your suggestion then." Based on this conversation, and your knowledge of GlobalCorp, select the best solution to the email problems in the network.}

Options:

A- After careful consideration you decide that you will implement secure email in a test group using X.509v3 digital certificates. You choose this since every user received their certificate during an earlier phase, and those certificates included the ability to be used for secure email. Using the X.509v3 certificates, you will configure each machine to use S\MIME. You go to each computer and open Outlook Express, which is the default client email program in the test group. You go to the Tools and Account option, selecting the Mail tab, and the properties for the email account. You select he Security Tab and in the submenu for the Signing Certificate you configure the certificate for the user's account. You select 3DES as the algorithm to use. You then check the Encrypt Contents And Attachments For All Outgoing Messages check box and the Digitally Sign All Outgoing Messages check box. You accept the default of including the digital id when sending signed messages and the default to add sender certificates to the user address book, and close the properties the email account. You show the user how to send and receive email, showing the Purple ribbon that indicates a signed message and the Orange lock that indicates an encrypted message.

B- After careful consideration you decide that you will implement secure email in a test group using PGP. You will use a full licensed version of PGP. You will go to each computer and you will install the full PGP on each system. Once installed, you will show each user how to create a PGP certificate by requesting the certificate from the CATool CA server you installed specifically for secure email. After the user has received a certificate, you associate that PGP certificate with their Windows domain user account.With the PGP certificate

associated with the user account, you show each user how to manage their key ring. You show them how to generate their key, and you configure all user key strength to be 2048 bits. Now that the user has a strong key and a PGP certificate, you configure the email client of each user. You explain that each user will have to install the public key of each other user in the network. You test this by sending an email from your laptop with your PGP certificate attached, and you have the user save the attachment to their Outlook folder. With the certificate saved, you show them how to send secure email to you. You receive the email on your laptop, and double-click the lock to show the user that the secure email message was successfully sent and received.

C- After careful consideration you decide that you will implement secure email in a test group using GPG. You have decided to use GPG to avoid any licensing conflicts that might occur if any user requires secure email exchange with another individual that is in a country with different cryptography laws. You will go to each computer and you will install GPG on each system. Once installed, you will show each user how to create the required directory structure, by typing the command: gpg --gen-key Once the directory structure is created, you will show each user how to generate the required files, by typing the command: gpg--gen-key Since you want very secure email, you configure each system to use 2048 bit key strength and you select DSA and ElGamal encryption. With GPG installed and configured, you show each user how to use their new secure email. You have them open Outlook and create a new message to you. Once the message is created, you have them select the Security drop-down list and choose both GPG Sign and GPG Encrypt, and then press send. You show them on your laptop that you receive the message. You press Reply, and on your laptop also select the Security drop-down menu, where you choose both GPG Sign and GPG Encrypt. The user receives the message, and you show that secure email was successfully sent and received.

D- After careful consideration you decide that you will implement secure email in a test group using PGP. You will use a full licensed version of PGP. You will go to each computer and you will install the full PGP on each system.Once installed, you will show each user how to create a PGP certificate by requesting the certificate from the MS Enterprise Root CA server you installed, and configured specifically for secure email certificates. After the user has received a certificate, you associate that PGP certificate with their Windows domain user account. With the PGP certificate associated with the user account, you show each user how to manage their key ring. You show them how to generate their key, and you configure all user key strength to be 2048 bits. Now that the user has a strong key and a PGP certificate, you configure the email client of each user. You explain that each user will have to install the public key of each other user in the network. You test this bysending an email from your laptop with your PGP certificate attached, and you have the user save

the attachment to their Outlook folder. With the certificate saved, you show them how to send secure email to you. You receive the email on your laptop, and double-click the lock to show the user that the secure email message was successfully sent and received.

E- After careful consideration you decide that you will implement secure email in a test group using X.509v3digital certificates. You choose this since every user received their certificate during an earlier phase, and those certificates included the ability to be used for secure email. You will configure each machine to use PGP, with the X.509v3 certificates option. You go to each computer and open Outlook Express, which is the default client email program in the testgroup. You go to the Tools and Account option, selecting the Mail tab, and the properties for the email account. You select he Security Tab and in the submenu for the Signing Certificate you configure the certificate for the user account. You select DSA and ElGamal as the cryptosystem to use. You then check the Encrypt Contents And Attachments For All Outgoing Messages check box and the Digitally Sign All Outgoing Messages check box. You accept the default of including the digital id when sending signed messages and the default to add sender certificates to the user address book, and close the properties the email account.You show the user how to send and receive email, showing the Purple ribbon that indicates a signed message and the Orange lock that indicates an encrypted message.

Answer:

A

Question 8

Question Type: MultipleChoice

Now that you have a fully functioning CA hierarchy in each location, and that the trusted network is well underway, you are called in to meet with Orange. Orange comes into the room, and you talk to one another for a while. It seems that now with the CA hierarchy in

place, you need to plan the certificate rollout for the individual users and computers in the network. Since this is the executive building, Orange places higher security requirements here than on the other buildings. Certificates need to be issued to all the entities, computers and users, in the network. Orange has decided that for all senior level management, the process for certificate issuance should be even more secure than the rest of the deployment. Based on this information, and you understanding of the GlobalCorp environment, choose the best solution to assigning certificates to the computers and users of the trusted network in the Executive building:}

Options:

A- You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network, followed by assigning certificates to the users in the network. For this task, you divide the other administrators into four teams, one per floor of the building. Each team will be responsible for the assigning of certificates to the computers and users on the corresponding floor. To make the process faster, you have decided to install a new CA for each floor. The team leader on each floor will install and configure the CA, and you will oversee the process. With the new CAs installed, one administrator from each team goes to each desk on the floor and makes a request for a certificate for the computer using Internet Explorer. Once the machine certificate is installed, the administrator has each user log on to their machine and the administrator walks the user through the process of connecting to the CA_SERVER\certsrv on their floor to request a user certificate. To ensure the security of the senior level management, you lead the team on the fourth floor. You install the new CA yourself, and oversee the configuration of the certificates for every machine and user on the floor.

B- You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1.You open Active Directory Users and Computers
2.You use Group Policy to edit the domain policy that is controlling the executive building.
3.You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.

4.In the template list, you select computer, and define CA as the location to send the request.
5.You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart. Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps: 1.Log on to your computer as your normal user account 2.Open Internet Explorer, and to connect to the CA_SERVER\certsrv. 3.Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request. 4.When the certificate is issued, click the Install This Certificate hyperlink on screen. Finally, you address the senior level management. For these people, you want the security to be higher, so you select a stronger algorithm for their certificates. With all the other certificates, you used the default key strength and algorithms. However, the senior level management needs higher security. Therefore, you personally walk each person through the process of requesting a certificate; only you ensure that they select 1024-bit AES as their encryption algorithm.

C- You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1.You open Active Directory Users and Computers
2.You use Group Policy to edit the domain policy that is controlling the executive building.
3.You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4.In the template list, you select computer, and define CA as the location to send the request.
5.You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart. Once you finishing setting up the computers to be assigned certificates, you shift your focus to the users, except for the senior management, in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:
1.Log on to your computer as your normal user account
2.Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3.Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request.

4.When the certificate is issued, click the Install This Certificate hyperlink on screen.
Finally, you address the senior level management in the building. For these people, you personally go into their office and walk through the steps with each person.
1.The user logs on to the computer with their normal user account
2.You open the MMC and add the personal certificates snap-in
3.You right-click certificates and Request A New Certificate
4.The user fills in the requested information, and you verify this information.
5.You put the certificate request onto a USB drive, and take the request back to the CA.
6.You put the USB drive into the CA, manually process the request, and put the issued certificate onto the USB drive.
7.You bring the USB drive back to each person, and manually import their new certificate

D- You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1.You open Active Directory Users and Computers
2.You use Group Policy to edit the domain policy that is controlling the executive building.
3.You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4.In the template list, you select computer, and define CA as the location to send the request.
5.You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart. Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps: 1.Log on to your computer as your normal user account 2.Open Internet Explorer, and to connect to the CA_SERVER\certsrv. 3.Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request. 4.When the certificate is issued, click the Install This Certificate hyperlink on screen.
Finally, you address the senior level management. For these people, you want the security to be higher, so you select a different certificate scheme. By using a different scheme, you ensure that there will be no possibility of other people in the building gaining access

to the senior level management accounts. For these accounts you utilize licensed PGP digital certificates that can be used for both authentication and secure email. You personally show each manager how to create and use their key ring, providing for very secure communication.

E- You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1.You open Active Directory Users and Computers
2.You use Group Policy to edit the domain policy that is controlling the executive building.
3.You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4.In the template list, you select computer, and define CA as the location to send the request.
5.You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart. Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:
1.Log on to your computer as your normal user account
2.Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3.Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request. 4.When the certificate is issued, click the Install This Certificate hyperlink on screen.

Answer:

C

Question 9

Question Type: MultipleChoice

You are well along your way to getting the MegaCorp security up to what you consider an acceptable level. You feel the security is now solid enough that you can go ahead and some new tests and perform analysis on the network. You plug in your laptop and fire up Snort to see the traffic coming into the network. You plug in on the outside of the router, to see the unfiltered traffic that the network must deal with. In full promiscuous mode, you collect data for an hour, to filter through it later. Since you captured quite a bit of data, you filter out a few specific lines to analyze. 10\27-23:48:42.126886 0:D0:9:7E:E5:E9 -> 0:D0:9:7F:C:9B type:0x800 len:0x3C

10.0.10.237 -> 10.0.10.234 ICMP TTL:128 TOS:0x0 ID:1185 IpLen:20 DgmLen:36 Type:8 Code:0 ID:3 Seq:289

ECHO =+= + 10\27-

23:48:42.137906 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3C

10.0.10.237 -> 10.0.10.235 ICMP TTL:128 TOS:0x0 ID:1186 IpLen:20 DgmLen:36 Type:8 Code:0 ID:3 Seq:290

ECHO =+= + 10\27-

23:48:42.148642 0:D0:9:7E:E5:E9 -> 0:D0:9:7E:F9:DB type:0x800 len:0x3C 10.0.10.237 -> 10.0.10.236 ICMP

TTL:128 TOS:0x0 ID:1187 IpLen:20 DgmLen:36 Type:8 Code:0 ID:3 Seq:291 ECHO

=+= + 10\27-

23:48:42.167031 0:D0:9:7E:E5:E9 -> 0:D0:9:68:87:2C type:0x800 len:0x3C

10.0.10.237 -> 10.0.10.238 ICMP TTL:128 TOS:0x0 ID:1190 IpLen:20 DgmLen:36 Type:8 Code:0 ID:3 Seq:292

ECHO =+= + 10\27-

23:48:42.177247 0:D0:9:7E:E5:E9 -> 0:D0:9:69:48:E3 type:0x800 len:0x3C

10.0.10.237 -> 10.0.10.239 ICMP TTL:128 TOS:0x0 ID:1191 IpLen:20 DgmLen:36 Type:8 Code:0 ID:3 Seq:293

ECHO =+= + 10\28-

19:09:07.387953 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:1

TCP TTL:44 TOS:0x0 ID:24652 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.320917 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:2

TCP TTL:44 TOS:0x0 ID:52330 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.377933 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:3

TCP TTL:44 TOS:0x0 ID:10807 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.328200 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:4

TCP TTL:44 TOS:0x0 ID:40192 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.363859 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:5

TCP TTL:44 TOS:0x0 ID:20497 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.391163 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:6

TCP TTL:44 TOS:0x0 ID:30756 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

19:09:07.300794 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C 10.0.10.236:57228 -> 10.0.10.235:7

TCP TTL:44 TOS:0x0 ID:3946 IpLen:20 DgmLen:40 ******** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

=+= + 10\28-

01:52:16.979681 0:D0:9:7E:E5:E9 -> 0:D0:9:7F:C:9B type:0x800 len:0x3E 10.0.10.237:1674 ->

10.0.10.234:31337 TCP TTL:128 TOS:0x0 ID:5277 IpLen:20 DgmLen:48 ******S* Seq: 0x3F2FE2CC Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:52:16.999652 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E 10.0.10.237:1675 ->

10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5278 IpLen:20 DgmLen:48 ******S* Seq: 0x3F30DB1F Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:52:17.019680 0:D0:9:7E:E5:E9 -> 0:D0:9:7E:F9:DB type:0x800 len:0x3E 10.0.10.237:1676 ->

10.0.10.236:31337 TCP TTL:128 TOS:0x0 ID:5279 IpLen:20 DgmLen:48 ******S* Seq: 0x3F3183AE Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:52:17.059669 0:D0:9:7E:E5:E9 -> 0:D0:9:68:87:2C type:0x800 len:0x3E 10.0.10.237:1678 ->

10.0.10.238:31337 TCP TTL:128 TOS:0x0 ID:5282 IpLen:20 DgmLen:48 ******S* Seq: 0x3F332EC2 Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:52:17.079821 0:D0:9:7E:E5:E9 -> 0:D0:9:69:48:E3 type:0x800 len:0x3E 10.0.10.237:1679 ->

10.0.10.239:31337 TCP TTL:128 TOS:0x0 ID:5283 IpLen:20 DgmLen:48 ******S* Seq: 0x3F3436FA Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:45:18.733562 0:D0:9:7E:E5:E9 -> 0:D0:9:7F:C:9B type:0x800 len:0x3E 10.0.10.237:1646 ->

10.0.10.234:12345 TCP TTL:128 TOS:0x0 ID:4974 IpLen:20 DgmLen:48 ******S* Seq: 0x38E326F7 Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:45:18.753691 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E 10.0.10.237:1647 ->

10.0.10.235:12345 TCP TTL:128 TOS:0x0 ID:4975 IpLen:20 DgmLen:48 ******S* Seq: 0x38E3D2D0 Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:45:18.773781 0:D0:9:7E:E5:E9 -> 0:D0:9:7E:F9:DB type:0x800 len:0x3E 10.0.10.237:1648 ->

10.0.10.236:12345 TCP TTL:128 TOS:0x0 ID:4976 IpLen:20 DgmLen:48 ******S* Seq: 0x38E4CF5C Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:45:18.813837 0:D0:9:7E:E5:E9 -> 0:D0:9:68:87:2C type:0x800 len:0x3E 10.0.10.237:1650 ->

10.0.10.238:12345 TCP TTL:128 TOS:0x0 ID:4979 IpLen:20 DgmLen:48 ******S* Seq: 0x38E692B6 Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + 10\28-

01:45:18.833772 0:D0:9:7E:E5:E9 -> 0:D0:9:69:48:E3 type:0x800 len:0x3E 10.0.10.237:1651 ->

10.0.10.239:12345 TCP TTL:128 TOS:0x0 ID:4980 IpLen:20 DgmLen:48 ******S* Seq: 0x38E7211C Ack: 0x0

Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+= + Looking at the types of traffic that are hitting your network, what types of attacks are you dealing with, and what is the best solution for mitigating those attacks?}

Options:

A- There is a clear attack pattern, where the attacker is looking for packets that are formed with a TTL of 128, followed by a TTL of 44. Finally, the attacker is looking to exploit the NOP SackOK vulnerability. To mitigate these attacks, you recommend implementing a new firewall on the outside of the router, designed with rules to specifically stop these attacks, allowing the rest of the traffic through to your router and the rest of your perimeter defense.

B- There is a clear pattern of attack, starting with general reconnaissance to see which systems are up and running to respond to attack inquiries. Next, the attacks show port scans, looking specifically for open ports on a unique host, and then moving to searching out NetBus and SubSeven servers. To mitigate these attacks, you do not recommend any new technology. You feel that your firewall, IDS, and routers will properly address these types of attacks.

C- Looking at the traffic, you are unable to identify any pattern of attack. You see normal legitimate traffic, the type of which you see every day. The traffic that you have captured provides you no clues as to the current attacks against your network, and as such you make no recommendations to mitigate.

D- There is a clear attack pattern, where the attacker first is checking to see which hosts will reply to sequential packets, followed by vulnerability checking for the IPLen:20 server vulnerability. To mitigate these attacks, you recommend reconfiguring the access control lists on the routers, specifically to address the IPLen:20 attack, and to address the sequential packet attack. You recommend that with the router configuration change, the threats will be properly addressed.

E- There is a clear pattern of attack, starting with the attacker looking for hosts that will respond to the ID:3 vulnerability. Once identified, the attacker runs a second set of scans, looking for hosts that are vulnerable to a TOS:0x0 attack, and finally running a scan to check for hosts that are vulnerable to the MSS: 1460 NOP attack. To mitigate these attacks, you recommend implementing a new firewall on the outside of the router, designed with rules to specifically stop these attacks, allowing the rest of the traffic through to your router and the rest of your perimeter defense.

Answer:

B

Question 10

Question Type: **MultipleChoice**

The MegaCorp network has been running smoothly for some time now. You are growing confident that you have taken care of all the critical needs, and that the network is moving towards a new state of maturity in the current configuration. You head out of the office on Friday at noon, since you have put in lots of long hours over the lat month. On Monday, you are driving into the office, and you happen to look at the speed limit sign that is on the road right next to MegaCorp. On the sign, in black paint, you see the following symbol:

Compaq)(128 Not good, you think, someone has been wardriving your office complex. That better not be in my office. The office building that MegaCorp is in has many other offices and companies, MegaCorp is not the only tenant. When you get inside, you check all your primary systems, router, firewall, and servers, looking for quick and fast signs of trouble. There does not seem to be any trouble so far. You check through your Snort logs, and so far so good. You are starting to think that whatever the war drivers found, it was not part of MegaCorp. You know that the MegaCorp policy does not allow for wireless devices, and you have neither installed nor approved any wireless for the network. Since it is still early (you get in at 7:30 on Mondays), you do not have anyone to talk to about adding any wireless devices. Select the solution that will allow you to find any unauthorized wireless devices in the network in the least amount of time, and with the least disruption to the office and employees.}

Options:

A- Since the company has a clear policy against the use of wireless devices, and since you know each employee you are fairly confident that the device in question is not inside the MegaCorp office. You schedule from 8:00 to 8:30 to do a visual walkthrough of the facilities. At 8:00, you grab your notebook, which has a network map and other reference notes, and you begin your walkthrough. You walk into every office, except for the CEO office, which is locked, and access is not granted. You spend several minutes in each office, and you spend some time in the open area where the majority of the employees work. You do not see any wireless access points, and you do not see any wireless antennas sticking up anywhere. It takes you more than the half an hour you allocated. By 9:00, the office has filled up, and most people are getting their workweek started. You see the CEO walking in, and motion that you have a question. You say, 'I am doing a quick walkthrough of the office, there might be a wireless device in here, and I know they are not allowed, so I am checking to see if I can find it.' 'As far as I know, there are no wireless devices in the network. We don't allow it, and I know that no one has asked me to put in wireless.' 'That what I thought. I sure we don't have any running here.' You reply. You are confident the wireless problem is in another office.

B- You decide to spend a full hour and a half from 8:00 to 9:30 going over your logs and data. Until then, you wrap up some early email and pull the log files together to review. It takes some time to gather all the log files that you can find, but you are able to get everything

you need. You get the log form the Router, the Firewall, the IDS, the internal servers, and the web and ftp server. For the next 90 minutes you do nothing other than study the logs looking for unusual traffic, or anything that would be a trigger to you that there has been an intruder in the network. First, you spend time on the router logs. On the routers you see a series of the following events:
%SYS-5-CONFIG_I:
Configured from console by vty1 (10.10.50.23) This is an event youconsider, and dismiss as not from an attacker. You then analyze the firewall, and again there you find that there are no logs indicating an intruder is present. All the IP traffic is from authorized IP Addresses. The IDS logs yield similar results. Only authorized traffic from hosts that have legitimate IP Addresses from the inside of the network. Analyzing the server's logs brings you to the same conclusion. All four severs show that the only access has been from the authorized hosts in the network, that no foreign IP Addresses have even attempted a connection into the private servers. The web\ftp server that has a public IP Address has had some failed attempts, but these are all in the realm of what you expect, nothing there stands out to you as well After your hour and half, you feel that you have gone through all the logs, and that there is no evidence that there has been any unauthorized access into any of your network resources, and you conclude that the wireless device is not in your office.

C- You take your laptop, which has a built-in wireless network card, and you enable it. You had not enabled the card before, as you know that wireless is not used in this network. You do a quick install of NetStumbler and watch on screen to see what might come up sitting in your office. A few seconds after the WNIC is initialized and NetStumbler is running, you see the following line in NetStumbler:
MAC:
46EAB5FD7C43, SSID:
Dell, Channel:
11, Type:
Peer, Beacon:
100. You expand channel 11 on the left side of NetStumbler, and see that MAC 46EAB5FD7C43 is bolded. You are surprised to find that there is a wireless device running in the network, and now you are off to see if you can locate the physical device. You take your laptop and head out of your office. You get about 20 feet away from the office when you are stopped by the HR director, who needs help with a laser printer. You also stop to chat about your findings with the CEO, who has just come in to the office. You put your laptop back in your office, to check later in the day. Although you did not isolate the physical location of the device, you are confident that you have indeed

found a rogue device. As soon as you locate the device, you will make a report for the CEO, and see to it that the device is removed immediately.

D- You take your laptop, initialize your WNIC, plug in your external antenna, and enable NetStumbler. You are glad that you keep all your gear nearby, even when you don normally use it. It is not yet 8:00, and you will be able to walk the office freely, looking for any rogue device. You turn on the laptop, and turn on your WNIC and NetStumbler. Right away, you see the following line:
MAC:
46EAB5FD7C43, SSID:
Dell, Channel:
11, Type:
Peer, Beacon:
100. You think that is what you were expecting, and you go on looking for the unauthorized device. You walk around the office for a while, and see no fluctuation in the numbers, and do not see any other devices on screen. By 8:30, most of the employees have come into the office. You meet the CEO, who is just coming into the office and give a short report on what you are doing. Everyone you meet has their lunches, work files, briefcases or laptop bags, and they get settled in like any other day. You get pulled into several conversations with your coworkers as they get started. At 9:10, you get back to your laptop and you look down at your screen to see what NetStumbler has to show. There are now two lines, versus the one that was there before:
MAC:
46EAB5FD7C4, SSID: Dell, Channel:
11, Type:
Peer, Beacon: 100. MAC:
000BCDA36ED, SSID:
Compaq, Channel: 9,
Type:
Peer, Beacon:
75. You close your laptop confident that you now know the exact location of the rogue device, which you have identified as a Compaq

laptop, running in peer mode, and you go to address the device immediately.

E- You take your laptop, initialize your WNIC, plug in your external antenna, and enable NetStumbler. You are glad that you keep all your gear nearby, even when you don normally use it. You would have had a 40 minute round trip drive to go home and get your own wardriving equipment. By 8:30 you have found several wireless devices, but are not sure which, if any might be in your office. The output from NetStumbler shows the following:
MAC:46EAB5FD7C43, SSID:Dell, Channel:11, Type:Peer, Beacon:100 MAC:AB3B3E23AB45, SSID:Cisco, Channel:9, Type:AP, Beacon:85 MAC:000625513AAE, SSID:Compaq, Channel:7, Type:Peer, WEP, Beacon:67 MAC:000C4119420F, SSID:Private, Channel:11, Type:AP, Beacon:55 The one you are most interested in is the Compaq device, as although you know the war drivers might have just written it down, you want to look for Compaq devices first. The Compaqis also an AP, so your suspicion is high. You walk around the office, watchingforthe numbers in NetStumbler to adjust. As you walk towards the street, you note the strength of the Compaq device weakens, by the time you get near the windows the signal is very weak. So, you turn around and walk away from the street, and sure enough the signal gets stronger. You actually walk out the main office door into the building interior courtyard. Across the courtyard you find the signal stronger and stronger. After you walk around for some time, you are sure that you have isolated the signal as coming from an office inside the building and exactly opposite MegaCorp. The device is not in your office, and you will report this to the CEO. You will also ask the CEO if you should inform the neighbor that their network is possibly at risk due to their wireless network use.

Answer:

D

Question 11

Question Type: MultipleChoice

Although you feel that you have taken solid steps in the security of MegaCorp, you would like to have some more analysis and documentation of the state of the network, and the systems in place protecting MegaCorp resources. The CEO wants to know what MegaCorp should be spending on securing these resources, and wants justification for the numbers that you provide. You inform the group that you will be able to provide them with a Risk Analysis on the defined resources, and you also suggest that MegaCorp perform a full business Risk Analysis, and that they make it part of their policy to perform ongoing analysis. During the first meeting after the agreement on analysis, a sales manager tells you the following; "We are rolling out a new online sales component to our organization. It will be up to you to design the system for this, but we anticipate it being up and running next month and are looking to have initial revenues of around $1,000 per day through that component." "All right," you respond "If the initial revenues are going to be around $1,000 per day, what are you projecting will be the daily revenue through this in 6 and 12 months?" The CEO answers this question, "Our projections are to have an average of about $2,000 per day in six months and $3,000 per day within a year." "And, what is this system going to be responsible for? By that I mean, is this just an order taking machine, is it tied into inventory, is it tied into shipping, and so on?" you ask. "Right now, and as far as the current plan goes, this is an order taking system. It will not be tied into any of our other systems." "Are we going to get a new Internet connection for this server, or is it going to run off the current connection we have? I recommend a new connection, but am curious to know if that has been considered." "I think we can stick with our current connection for the time being. If it seems like there is a need in the future for the expenses of a new connection, we can discuss it then. Anything else?" "Not right now, as issues come up I will talk to you about them." The rest of the meeting does not require your attendance, so you head back to your office. Based on your knowledge of the MegaCorp environment, select the solution that best allow you to justify the expense of protecting the new server.}

Options:

A- You decide to perform a Quantitative Risk Analysis on the server. You meet with the sales director to find out that the server will only hold a copy of the catalog. You estimate that since the system will be directly connected with a public IP Address, and since it will hold customer data that it is a likely target for attack. You know that you have solid security systems in place, but you think there will be a

legitimate attack to compromise this server at least once per month. Based on this information you decide that the ARO is 12, and the SLE will be one day of operation plus one day to restore the system, therefore $6,000. With an ARO of 12, and with a SLE of $6,000 you determine that the ALE for the system is $72,000. You report to the CEO that although the current security systems in place are solid, this server requires security of it??s own. You identify the $72,000 that could be lost every year due to attacks, and request resources to properly protect the server. B. You decide to perform a Qualitative Risk Analysis on the new server. You organize a short meeting with the sales director to get a better idea of what will be stored on the system. You know the projected sales volumes, and you find out that on the system will be nothing more than a catalog, where people can order MegaCorp products. Since there is nothing of value stored on the server, you decide that the Level of Damage that would happen if this system is compromised is low and that the Likelihood of an Attack to gain access is low. Since the company needs the system for sales, you decide that the threat of a power loss is significant. Your report back to the CEO is that the current security systems in place are adequate for the new system, that it will be protected by the firewall and IDS. You do request to increase the resources for power equipment, specifically a large battery backup for the server.

C- You decide to follow the Facilitated Risk Analysis Process (FRAP) for the server. You sit down in your office by yourself, and you list out the vulnerabilities that might exist for the server. You then categorize those vulnerabilities into High, Medium, and Low. Taking each individual vulnerability that you discovered, you further detail that listing the degree of impact that vulnerability could have, again categorizing them as High, medium, and Low. When you are done, you have a list that shows five vulnerabilities, only one of them High, and that is attempted system compromise. You have identified this vulnerability to have a Low impact, since it will only contain the MegaCorp catalog and no other critical services. You report back to the CEO that the current systems in place are adequate, and your only suggestion is to possibly increase the power backup to a larger model for the server.

D- Since this is the only system that you are requested to analyze, and the CEO is looking for numbers, you decide to run a fast Qualitative Risk Analysis. You know that the server is going to generate $6,000 per month, and you think there will most likely be an attack on the server at least twice a month. This means that for this server, you have an SLE of $6,000 and an ALE of 24. With an SLE of $6,000, and with an ALE of 24, you determine that the SRO for the system is $144,000. You report to the CEO that there is a risk of $144,000 to this server every year, and you recommend that for the first year that full risk amount be spent on mitigating the risk, so that in subsequent years you can report the risk has been reduced to zero.

E- With only this one single system to analyze, you decide that a Quantitative Risk Analysis is appropriate. You identify three major

threats:
Power Outage, Administrator-level system compromise, and Denial of Service attacks. You assign the power outage a low likelihood, the administrative compromise a medium likelihood, and the DoS a high likelihood. You assign the power outage a high level of damage, you assign the administrative compromise a high level of damage, and you assign the DoS a low level of damage. Since the likelihood of the power outage is low, you do not recommend spending any new money on this in your report to the CEO. Since the level of damage is so high due to the administrative compromise, you recommend new security systems to protect against that threat. You recommend that the systems in place to mitigate the threat of the administrative compromise also be capable of addressing the DoS threat.

Answer:

A

Question 12

Question Type: MultipleChoice

Now that you have MegaCorp 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 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 forwhatever 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. "Il 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. 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 MegaCorp network up to this point, choose the best solution for the secure remote user needs:}

Options:

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 its lf is configured to exchange keys with the user ISP to create a tunnel between the user ISP endpoint and the MegaCorp 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 redirection to the inside network, with all resources available in his or her Network Neighborhood.

C- 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

D- 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.

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:

C