Free Questions for SC0-502 by go4braindumps

Shared by Benjamin on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Blue thanks you for your plan and design and took it into consideration. You are then informed that Orange has gone ahead and made a new plan, which will incorporate some of your suggestions, but is going to build the network a bit differently. In Testbed and in each remote office there will be a single self-sufficient CA hierarchy, one that is designed to directly integrate with the existing network. Orange mentions that the hierarchy is only to go two-levels deep, you are not to make an extensive hierarchy in any location. This means a distinct CA hierarchy in six locations, inclusive of the Testbed headquarters. Using this information, choose the solution that will provide for the proper rollout of the Certificate Authorities in the network.}

Options:

A- In each location, you recommend the following steps: 1.Harden a system to function as the Root CA
2.Harden a system to function as the Registration Authority 3.Configure CATool on the Root CA
4.Configure CATool on the Registration Authority, as a subordinate to the Root CA 5.Once the Subordinate CA is active, take the Root CA offline
6.Configure users for the CAs 7.Configure each Root CA to trust each other Root CA via cross certification 8.Test the CA hierarchy
9.Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

B- In each location, you recommend the following steps: 1.Harden a system to function as the Root CA
2.Harden a system to function as a Registration Authority
3.Configure a Windows Enterprise Root CA

4.Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification 5.Configure a Windows Stand-Alone Subordinate Enrollment Authority to function as the Registration Authority
6.Once the Stand-Alone Subordinate is installed, take the Enterprise Root CA offline
7.Test the CA hierarchy 8.Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

C- In each location, you recommend the following steps: 1.Harden a system to function as the Root CA
2.Harden a system to function as the Registration Authority
3.Configure a Windows Enterprise Root CA
4.Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification
5.Configure a Windows Enterprise Registration Authority, as a subordinate to the Enterprise Root CA
6.Once the Subordinate CA is active, take the Enterprise Root CA offline
7.Test the CA hierarchy7.Test the CA hierarchy 8.Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

D- In each location, you recommend the following steps:
1.Harden a system to function as the Root CA
2.Harden a system to function as the Registration Authority
3.Configure a Windows Enterprise Root CA
4.Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification
5.Configure a Windows Registration Authority, as a subordinate to the Enterprise Root CA
6.Test the CA hierarchy 7.Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

E- In each location, you recommend the following steps:
1.Harden a system to function as the Root CA
2.Harden a system to function as the Registration Authority

3.Configure CATool on the Root CA
4.Configure CATool on the Registration Authority, as a subordinate to the Root CA
5.Configure users for the CAs
6.Configure each Root CA to trust each other Root CA via cross certification
7.Test the CA hierarchy
8.Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

Answer:

D

Question 2

Question Type: MultipleChoice

GlobalCorp is a company that makes state of the art aircraft for commercial and government use. Recently GlobalCorp has been working on the next generation of low orbit space vehicles, again for both commercial and governmental markets. GlobalCorp has corporate headquarters in Testbed, Nevada, USA. Testbed is a small town, with a population of less than 50,000 people. GlobalCorp is the largest company in town, where most families have at least one family member working there. The corporate office in Testbed has 4,000 total employees, on a 40-acre campus environment. The largest buildings are the manufacturing plants, which are right next to the Research and Development labs. The manufacturing plants employee approximately 1,000 people and the RD labs employ 500 people. There is one executive building, where approximately 500 people work. The rest of the employees work in Marketing, Accounting, Press

and Investor Relations, and so on. The entire complex has a vast underground complex of tunnels that connect each building. All critical functions are run from the Testbed office, with remote offices around the world. The remote offices are involved in marketing and sales of GlobalCorp products. These offices also perform maintenance on the GlobalCorp aircraft and will occasionally perform RD and on-site manufacturing. There are 5 remote offices, located in:

New York, California, Japan, India, and England. Each of the remote offices has a dedicated T3 line to the GlobalCorp HQ, and all network traffic is routed through the Testbed office the remote offices do not have direct Internet connections. You had been working for two years in the New York office, and have been interviewing for the lead security architect position in Testbed. The lead security architect reports directly to the Chief Security Officer (CSO), who calls you to let you know that you got the job. You are to report to Testbed in one month, just in time for the annual meeting, and in the meantime you review the overview of the GlobalCorp network: Your first day in GlobalCorp Testbed, you get your office setup, move your things in place, and about the time you turn on your laptop, there is a knock on your door. It is Orange, the Chief Security Officer, who informs you that there is a meeting that you need to attend in a half an hour. With your laptop in hand, you come to the meeting, and are introduced to everyone. Orange begins the meeting with a discussion on the current state of security in GlobalCorp. "For several years now, we have constantly been spending more and more money on our network defense, and I feel confident that we are currently well defended." Orange, puts a picture on the wall projecting the image of the network, and then continues, "We have firewalls at each critical point, we have separate Internet access for our public systems, and all traffic is routed through our controlled access points. So, with all this, you might be wondering why I have concern." At this point a few people seem to nod in agreement. For years, GlobalCorp has been at the forefront of perimeter defense and security. Most in the meeting are not aware that there is much else that could be done. Blue continues, "Some of you know this, for the rest it is new news: MassiveCorp is moving their offices to the town right next to us here. Now, as you all know, MassiveCorp has been trying to build their orbital systems up to our standards for years and have never been able to do so. So, from a security point of view, I am concerned." This is news to most people, Yellow, the Vice President of Research asks, "We have the best in firewalls, we have the best in you and your systems, what are you suggesting?" The meeting continues for some time, with Orange leading the discussion on a whole new set of technologies currently not used in the network. After some time, it is agreed upon that GlobalCorp will migrate to a trusted networking environment. The following week, Orange informs you that you will be working directly together on the development of the planning and design of the trusted network. The network is going to run a full PKI, with all clients and servers in the network using digital certificates.

You are grateful that in the past two years, Orange has had all the systems changed to be running only Windows 2000, both server and professional systems, running Active Directory. You think the consistent platform will make the PKI roll out easier. The entire GlobalCorp network is running Active Directory, with the domain structure as in the following list: Testbed.globalcorp.org Newyork.globalcorp.org California.globalcorp.org Japan.globalcorp.org India.globalcorp.org England.globalcorp.org Although you will be working in the Testbed office, the plan you develop will need to include the entire GlobalCorp organization. Based on this information, select the solution that describes the best plan for the new trusted network of GlobalCorp:}

Options:

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

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

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

C- You design the plan for two weeks, and then you present it to Orange. Your plan follows these critical steps: 1.Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS. 2.Draft a CPF based on your own guidelines, including physical and technology controls. 3.Design the system, outside of the executive office, to be a full hierarchy, with the Root CA for the hierarchy located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA. 4.In the executive building, you design the system to be a mesh CA structure, with one CA per floor of the building. 5.Design the hierarchy with each remote office and building having it own enrollment CA. 6.Build a small test pilot program, to test the hierarchy, and integration with the existing network. 7.Implement the CA hierarchy in the executive office, and get all users acclimated to the system. 8.Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system. 9.One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system. 10.Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network. 11.Evaluate the rollout, test, and modify as needed to improve the overall security of the GlobalCorp trusted network.

D- You design the plan for two weeks, and then you present it to Orange. Your plan follows these critical steps: 1.Draft a Certificate Policy (CP) document to define what users will be allowed to do with their certificates, and a Certification Practice Statement (CPS)

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

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

Answer:

B

Question 3

Question Type: MultipleChoice

It has been quite some time since you were called in to address the network and security needs of MegaCorp. You feel good in what you have accomplished so far. You have been able to get MegaCorp to deal with their Security Policy issue, you have secured the router, added a firewall, added intrusion detection, hardened the Operating Systems, and more. One thing you have not done however, is run active testing against the network

from the outside. This next level of testing is the final step, you decide, in wrapping up this first stage of the new MegaCorp network and security system. You setup a meeting with the CEO to discuss. "We have only one significant issue left to deal with here at MegaCorp," you begin. "We need some really solid testing of our network and our security systems." "Sounds fine to me, don't you do that all the time anyway? I mean, why meet about this?" "Well, in this case, I'd like to ask to bring in outside help. Folks who specialize in this sort of thing. I can do some of it, but it is not my specialty, and the outside look in will be better and more independent from an outside team." "What does that kind of thing cost, how long will it take?" "It will cost a bit of money, it won't be free, and with a network of our size, I think it can be done pretty quick. Once this is done and wrapped up, I will be resigning as the full time security and network pro here. I need to get back to my consulting company full time. Remember, this was not to be a permanent deal. I can help you with the interview, and this is the perfect time to wrap up that transition." "All right, fair enough. Get me your initial project estimates, and then I can make a more complete decision. And, Il get HR on hiring a new person right away." Later that afternoon you talk to the CEO and determine a budget for the testing. Once you get back to your office, you are calling different firms and consultants, and eventually you find a consulting group that you will work with. A few days later you meet with the group in their office, and you describe what you are looking for, and that their contact and person to report to is you. They ask what is off limits, and your response is only that they cannot do anything illegal, to which they agree and point out is written in their agreement as well. With this outside consulting group and your

knowledge of the network and company, review and select the solution that will best provide for a complete test of the security of MegaCorp.}

Options:

A- The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports. The consultants will first run remote network surveillance to identify hosts, followed by port scans and both passive and active fingerprinting. They will then run vulnerability scanners on the identified systems, and attempt to exploit any found vulnerabilities. They will next scan and test the router and firewall, followed by testing of the IDS rules They will then perform physical surveillance and dumpster diving to learn additional information. This will be followed by password sniffing and cracking. Finally, they will call into MegaCorp to see what information they can learn via social engineering.

B- The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports. The first thing the consultants will do is dumpster diving and physical surveillance, looking for clues as to user information and other secret data that should not be outside of the network. Once they have identified several targets through the dumpster diving, they will run scans to match up and identify the workstations for those users. After identifying the user workstations, they will run vulnerability checks on the systems, to find holes, and if a hole is found they have been given permission to exploit the hole and gain access of the system.They will attempt to gain access to the firewall and router remotely, via password guessing, and will test the response of the network to Denial of Service attacks. Finally, they will call into MegaCorp to see what information they can learn via social engineering.

C- The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports The consultants surprise you with their initial strategy. They intend to spend nearly 100% of their efforts over the first week on social engineering and other physical techniques, using little to no technology. They have gained access to the building as a maintenance crew, and will be coming into the office every

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

D- The consulting group has identified the steps it will follw in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports. The consultants have decided on a direct strategy. They will work inside the MegaCorp office, with the group introducing themselves to the employees. They will directly interview each employee, and perform extensive physical security checks of the network. They will review and provide analysis on the security policy, and follow that with electronic testing. They will run a single very robust vulnerability scanner on every single client and server in the network, and document the findings of the scan.

E- The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.The consultants will start the process with remote network surveillance, checking to see what systems and services areavailable remotely. They will run both passive and active fingerprinting on any identified system. They will run customized vulnerability scanners on the identified systems, and follow that through with exploits, including new zero-day exploits they have written themselves. They will next run scans on the router, firewall, and intrusion detection, looking to identify operating systems and configurations of these devices. Once identified, they will run customized scripts to gain access to these devices. Once they complete the testing on the systems, they will dumpster dive to identify any leaked information.

Answer:

A

Question 4

Question Type: MultipleChoice

You go back through your notes to the day that you recommended that the company get a firewall in place. Red had been convinced that the ISP protected the network, and that a firewall was too much technology on top of the router. Now that you have been given this responsibility, and since you have configured the router already, you wish to get the firewall in place as quickly as possible. You meet quickly with the CEO and mention that the network currently has no firewall, a serious problem. You inform the CEO that this must be fixed immediately, and that you have several firewall options. For this one instance, the CEO tells you to build the best solution; the decision is not going to be based on direct cost. Based on your knowledge of and the information you have from MegaCorp, select the best solution to th organization firewall problem:}

Options:

A- You decide to take advantage of the features of Microsoft ISA Server and Checkpoint NG. You implement two firewalls, each with two network cards. From one Ethernet interface of the router, you connect to a Checkpoint firewall, and from the other Ethernet interface on the router, you connect to a Microsoft ISA firewall.The Checkpoint firewall is connected via one NIC to the router, and the other NIC is connected to the Web and FTP Server. The Microsoft ISA Server is connected via one NIC to the router and the other NIC is connected to the LAN switch. You perform the following steps and configurations to setup the firewalls:
1.First, you configure the IP Address on both network cards of both firewalls.
1, SMART Clients, and Policy Server as the only components to install and complete the installation of Checkpoint.
2.Second, you select the Floodgate-
3.Third, you configure the Checkpoint firewall so only Web and FTP traffic are allowed inbound.
4.Fourth, you select the Cache Mode option during the install of ISA Server and complete the installation of Microsoft ISA Server.
5.Fifth, you allow all outbound traffic through the ISA Server.
6.Sixth, you allow only inbound traffic through the ISA Server that is in response to outbound requests.

B- After analysis, you decide to implement a firewall using Checkpoint NG. You begin by installing a new machine, with a fresh hard drive, and the loading of NG. The new firewall will have four NICs. You connect the two Ethernet interfaces on the routers to two of the firewall NICs. You connect one firewall NIC to the Web and FTP server and one firewall NIC to the LAN switch. You perform the following steps and configurations to setup the firewall:
1.First, you configure the IP Addresses on all four network cards of the Checkpoint firewall.
2.Second, you select only the VPN-1 Firewall-1 components to install and complete the installation of Checkpoint.
3.Third, you configure the only new inbound network traffic to be destined for the WWW and FTP services on the Web and FTP server
4.Fourth, you block all other incoming traffic. 5.Fifth, you create anti-spoofing rules to block inbound traffic that might be spoofed. 6.Sixth, you configure all traffic to be allowed in the outbound direction

C- After you analyze the network, you have decided that you are going to implement a firewall using Microsoft ISA Server. The new firewall will have four NICs. You connect the two Ethernet interfaces on the routers to two of the firewall NICs. You connect one NIC to the Web and FTP server and one NIC to the LAN switch.You perform the following steps and configurations to setup the firewall:
1.First, you format a new hard drive and install a new copy of Windows 2000 Server. 2.Second, you configure the correct IP Addresses on the four network cards. 3.Third, you install ISA Server into Firewall only mode, and complete the installation. 4.Fourth, you configure all inbound traffic to require the SYN flag to be set, all other inbound network traffic is denied 5.Fifth, you configure the network card towards the Web and FTP server will only allow ports 80, 20, and 21. 6.Sixth, you configure all outbound traffic to be allowed.

D- After you analyze the company, you decide to implement a firewall using Microsoft ISA Server. You create a DMZ with the Web and FTP server on the network segment between the router and the new firewall. The firewall will have two NICs, one connected to the router, and one connected to the LAN switch You perform the following steps and configurations to setup the firewall:
1.First, you install a new version of ISA Server, installed in Firewall mode.
2.Second, you configure the inbound network card to disallow all network traffic that did not originate from inside the network or from the Web and FTP Server.
3.Third, you configure anti-spoofing rules to prevent spoofing attacks.
4.Fourth, you configure all outbound traffic to be allowed.
5.Fifth, you configure inbound traffic with the SYN flag on to be allowed, and to be logged to a SYSLOG server inside the network.

E- After you run an analysis on the network and the MegaCorp needs, you decide to implement a firewall using Checkpoint NG. The firewall will have three NICs. One NIC is connected to the router, one NIC is connected to the Web and FTP server and one NIC is connected to the LAN switch. You perform the following steps and configurations to setup the firewall:
1.First, you install a new version of Checkpoint NG, selecting the VPN-1 and Firewall-1 components, and complete the installation.
2.Second, you configure the inbound rules to allow only SYN packets that are destined for ports 80, 20, and 21 on the Web and FTP server.
3.Third, you disallow all inbound traffic for the internal network, unless it is in response to an outbound request. 4.Fourth, you configure anti-spoofing rules on the inbound interface and log those connections to a log server.

Answer:

E

Question 5

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 have decided 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 I cannot 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 going off, and just end up wasting everyone time." "That's a fair concern, but it is my concern. When we implement the system, I will fine tune it and adjust it until the alarms it generates are appropriate, and are generated when there is legitimately something to be concerned about. We are concerned with traffic that would indicate an attack; only then will the system send me an alert." For a few minutes there was talk back and forth in the room, and then the CEO responds again to your inquiry, "I agree that this type of thing could be helpful. But, we simply don't have any ore budget for it. Since it is a good idea, go ahead nd find a way to implement this, but don't spend ny money on it." ith this information, and your knowledge of MegaCorp, choose the answer that will provide the best olution 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 to ou 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;) Log 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 you alerts when ppropriate. 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 that machine. The achine logs all intrusions locally, and you will connect to the machine emotely ce 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 rule base: Alert tcp any any <> any 80 Alert 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 ew install of indows on a clean hard drive. ou install ISS Internet Scanner and ISS System Scanner

on the new system. System Scanner is configured to o full backdoor testing, full baseline testing, and full password testing. nternet Scanner is configured with a custom policy you made to scan for all vulnerabilities. You configure both canners to enerate automatic weekly reports and to send you alerts when n incident of note takes lace on the network. .

D- You install two computers to run your IDS. One will be a dedicated machine that is on the outside of the outer, and the second will be on the inside of the outer. You configure the achine on the outside of the router to run Snort, and you combine the default rules of several of the built-in ule sets. You combine the ddos.rules, os.rules, exploit.rules, icmp.rules, nd scan.rules. n the system that is inside the router, running Snort, you also combine several of the uilt-in rule sets. You ombine the scan.rules, web-cgi.rules, ftp.rules, web-misc.rules, and eb-iis.rules. ou configure the alerts on the two systems to send you email messages when events are dentified. After you mplement the two systems, you run some external scans and tests using vulnerability checkers and exploit testing software. You modify your rules based on your tests.

E- You install Snort on a dedicated machine just inside the router. The machine is designed to send alerts to you when appropriate. You do have some concern that the system will have too many rules to operate efficiently. To address this, you decide to pull the critical rules out of the built-in rule sets, and create one simple rule set that is short and will cover all of the serious incidents that the network might experience. alert udp any 19 <> $HOME_NET 7 (msg:'DOS UDP Bomb'; classtype:attempted-dos; sid:271; rev:1;) alert 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;) alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:'ICMP PING NMAP'; dsize: 0; itype: 8; classtype:attempted-recon; sid:469; rev:1;) alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:'SCAN XMAS';flags:SRAFPU; classtype:attempted-recon; sid:625; rev:1;) alert tcp $HOME_NET 31337 -> $EXTERNAL_NET 80 (msg:'SCAN synscan microsoft'; id: 39426; flags: SF; classtype:attempted-recon; sid:633; rev:1;)

Answer:

D

Question 6

Question Type: MultipleChoice

You go back through your notes to the day that you recommended that the company get a firewall in place. Purple had been convinced that the ISP protected the network, and that a firewall was too much technology on top of the router. Now that you have been given this responsibility, and since you have configured the router already, you wish to get the firewall in place as quickly as possible. You meet quickly with the CEO and mention that the network currently has no firewall, a serious problem. You inform the CEO that this must be fixed immediately, and that you have several firewall options. For this one instance, the CEO tells you to build the best solution; the decision is not oing to be based on direct cost. ased on your knowledge of and the information you have from MegaCorp, elect the best solution to the rganization firewall problem:} A. You decide to take advantage of the features of Microsoft ISA Server and Checkpoint NG. You implement wo firewalls, each with two network cards. From one Ethernet nterface of the outer, you connect to a Checkpoint firewall, and from the other Ethernet interface on the router, you connect to Microsoft ISA firewall. he Checkpoint firewall is connected via one NIC to the router, and the other NIC is nnected to the Web and TP Server. The Microsoft ISA Server is connected via one NIC o he router nd the other NIC is connected to the LAN switch. ou perform the following steps and configurations to setup the firewalls:

1.First, you configure the IP Address on both network cards of both firewalls.

2.Second, you select the Floodgate-1, SMART Clients, and Policy Server as the only components to install and omplete the installation of Checkpoint.

3.Third, you configure the Checkpoint firewall so only Web and FTP traffic are allowed inbound.

4.Fourth, you select the Cache Mode option during the install of ISA Server and complete the installation of icrosoft ISA Server. 5.Fifth, you allow all outbound traffic through the ISA Server. 6.Sixth, you allow only inbound traffic through the ISA Server that is in response to outbound requests.

Options:

B- After analysis, you decide to implement a firewall using Checkpoint NG. You begin by installing a new achine, with a fresh hard drive, and the loading of NG. The new irewall will have our NICs. You connect the two Ethernet interfaces on the routers to two f the firewall NICs. You connect one irewall NIC to the Web and FTP server and one firewall NIC to the LAN witch. ou perform the following steps and configurations to setup the firewall:

.First, you configure the IP Addresses on all four network cards of the heckpoint firewall. 2.Second, you select only the VPN-1 Firewall-1 components to install and complete the installation of heckpoint. 3.Third, you configure the only new inbound network traffic to be destined for the WWW and FTP services on he Web and FTP server 4.Fourth, you block all other incoming traffic. 5.Fifth, you create anti-spoofing rules to block inbound traffic that might be spoofed.

6.Sixth, you configure all traffic to be allowed in the outbound direction C. After you analyze the network, you have decided that you are going to implement a firewall using icrosoft ISA Server. The new firewall will have four NICs. You connect he wo Ethernet nterfaces on the routers to two of the firewall NICs. You connect one NIC to he Web and FTP server and one IC to the LAN switch. ou perform the following steps and configurations to setup the firewall:

1.First, you format a new hard drive and install a new copy of Windows 2000 Server. 2.Second, you configure the correct IP Addresses on the four network cards. 3.Third, you install ISA Server into Firewall only mode, and complete the installation. 4.Fourth, you configure all inbound traffic to require the SYN flag to be set, all other inbound network traffic is enied 5.Fifth, you configure the network card towards the Web and FTP server will only allow ports 80, 20, and 21. 6.Sixth, you configure all outbound traffic to be allowed.

D- After you run an analysis on the network and the MegaCorp needs, you decide to implement a firewall sing Checkpoint NG. The firewall will have three NICs. One NIC is onnected to the uter, one NIC is connected to the Web and FTP server and one NIC is connected to the AN switch. ou perform the following steps and configurations to setup the firewall:

1.First, you install a new version of Checkpoint NG, selecting the VPN-1 and Firewall-1 components, and omplete the installation.

2.Second, you configure the inbound rules to allow only SYN packets that are destined for ports 80, 20, and 21 n the Web and FTP server. 3.Third, you disallow all inbound traffic for he internal network, unless it is in response to an outbound equest. 4.Fourth, you

configure anti-spoofing rules on the inbound interface and log those connections to a log server.

E- After you analyze the company, you decide to implement a firewall using Microsoft ISA Server. You create DMZ with the Web and FTP server on the network segment etween the router nd the new firewall. The firewall will have two NICs, one connected to the router, and one connected to the LAN switch. ou perform the following steps and configurations to setup the firewall:
First, you install a new version of ISA Server, installed in Firewall mode.
2.Second, you configure the inbound network card to disallow all network traffic that did not originate from nside the network or from the Web and FTP Server. 3.Third, you configure anti-spoofing rules to prevent spoofing attacks. 4.Fourth, you configure all outbound traffic to be allowed. 5.Fifth, you configure inbound traffic with the SYN flag on to be allowed, and to be logged to a SYSLOG erver inside the network.

Answer:

D

Question 7

Question Type: **MultipleChoice**

For three years you have worked with MegaCorp doing occasional network and security consulting. MegaCorp is a small business that provides real estate listings and data to realtors in several of the surrounding states. The company is open for business Monday through Friday from 9 am to 6 pm, closed all evenings and weekends. Your work there has largely consisted of advice and planning, and you have been frequently disappointed by the lack of execution and follow through from the full time staff. On Tuesday, you received a call from MegaCorp's HR director, "Hello, I'd like to inform you that Purple (the full time senior network administrator) is no longer with us,

and we would like to know if you are interested in working with us full time." You currently have no other main clients, so you reply, "Sure, when do you need me to get going?" "Today," comes the fast and direct response. Too fast, you think. " What is the urgency, why can this wait until tomorrow?" "Red was let go, and he was not happy about it. We are worried that he might have done something to our network on the way out." "OK, let me get some things ready, and Il be over there shortly." You knew this would be messy when you came in, but you did have some advantage in that you already knew the network. You had recommended many changes in the past, none of which would be implemented by Purple. While pulling together your laptop and other tools, you grab your notes which have an overview of the network:

MegaCorp network notes:

Single Internet access point, T1, connected to MegaCorp Cisco router. Router has E1 to a private web and ftp server and E0 to the LAN switch. LAN switch has four servers, four printers, and 100 client machines. All the machines are running Windows 2000. Currently, they are having their primary web site and email hosted by an ISP in Illinois. When you get to MegaCorp, the HR Director and the CEO, both of whom you already know, greet you. The CEO informs you that Purple was let go due to difficult personality conflicts, among other reasons, and the termination was not cordial. You are to sign the proper employment papers, and get right on the job. You are given the rest of the day to get setup and running, but the company is quite concerned about the security of their network. Rightly so, you think, if these guys had implemented even half of my recommendations this would sure be easier.You get your equipment setup in your new oversized office space, and get started. For the time you are working here, your IP Address is 10.10.50.23 with a mask of \16. One of your first tasks is to examine the router configuration. You console into the router, issue a show running-config command, and get the following output:

MegaOne#show running-config Building configuration Current configuration:

! version 12.1 service udp-small-servers service tcp-small-servers ! hostname MegaOne ! enable secret 5 $1$7BSK3$H394yewhJ45JAFEWU73747. enable password clever ! no ip name-server no ip domain-lookup ip routing ! interface Ethernet0 no shutdown ip address 2.3.57.50 255.255.255.0 no ip directed broadcast ! interface Ethernet1 no shutdown ip 10.10.40.101 255.255.0.0 no ip directed-broadcast ! interface Serial0 no shutdown ip 1.20.30.23 255.255.255.0 no ip directed-broadcast clockrate

1024000 bandwidth 1024 encapsulation hdlc ! ip route 0.0.0.0 0.0.0.0 1.20.30.45 ! line console 0 exec-timeout 0 0 transport input all line vty 0 4 password remote login ! End After analysis of the network, you recommend that the router have a new configuration. Your goal is to make the router become part of your layered defense, and to be a system configured to help secure the network. You talk to the CEO to get an idea of what the goals of the router should be in the new configuration. All your conversations are to go through the CEO; this is whom you also are to report to. "OK, I suggest that the employees be strictly restricted to only the services that they must access on the Internet." You begin. "I can understand that, but we have always had an open policy. I like the employees to feel comfortable, and not feel like we are watching over them all the time. Please leave the connection open so they can get to whatever they need to get to. We can always reevaluate this in an ongoing basis." "OK, if you insist, but for the record I am opposed to that policy." "Noted," responds the CEO, somewhat bluntly. "All right, let see, the private web and ftp server have to be accessed by the Internet, restricted to the accounts on the server. We will continue to use the Illinois ISP to host our main web site and to host our email. What else, is there anything else that needs to be accessed from the Internet?" "No, I think that's it. We have a pretty simple network, we do everything in house." "All right, we need to get a plan in place as well right away for a security policy. Can we set something up for tomorrow?" you ask. "Let me see, Il get back to you later." With that the CEO leaves and you get to work. Based on the information you have from MegaCorp; knowing that the router must be an integral part of the security of the organization, select the best solution to the organization's router problem:}

Options:

A- You backup the current router config to a temp location on your laptop. Sunday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21 MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established MegaOne(config)#access-list 175 permit ip any

10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255 MegaOne(config)#interface Ethernet 0 MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable MegaOne(config)#interface Ethernet 1 MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable MegaOne(config-if)#^Z MegaOne#

B- You backup the current router config to a temp location on your laptop. Early Monday morning, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21 MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255 MegaOne(config)#interface Serial 0 MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no cdp enable MegaOne(config-if)#no ip directed broadcast MegaOne(config-if)#no ip unreachables MegaOne(config-if)#^Z MegaOne#

C- As soon as the office closes Friday, you get to work on the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21 MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255 MegaOne(config)#interface Ethernet 0 MegaOne(config-if)#ip access-group 175 in MegaOne(config)#interface Ethernet 1 MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#^Z MegaOne#

D- With the office closed, you decide to build the new router configuration on Saturday. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal MegaOne(config)#no cdp run MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60

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

E- You backup the current router config to a temp location on your laptop. Friday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration: MegaOne#configure terminal MegaOne(config)#no cdp run MegaOne(config)#no ip source-route MegaOne(config)#no ip finger MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20 MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21 MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established MegaOne(config)#access-list 175 deny ip 0.0.0.0 255.255.255.255 any MegaOne(config)#access-list 175 deny ip 10.0.0.0 0.255.255.255 any MegaOne(config)#access-list 175 deny ip 127.0.0.0 0.255.255.255 any MegaOne(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 any MegaOne(config)#access-list 175 deny ip 192.168.0.0 0.0.255.255 any MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255 MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255 MegaOne(config)#interface serial 0 MegaOne(config-if)#ip access-group 175 in MegaOne(config-if)#no ip directed broadcast MegaOne(config-if)#no ip unreachables MegaOne(config-
if)#^Z MegaOne#

Answer:

E

Question 8

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 Blue to meet in the conference room. When you get there, Blue 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," Blue tells you. "Wel Il let you two sort this out. Blue, do let me know when it's all ready to go." With that the VP leaves. You sit down across from Blue, 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 a laptop that uses an ORiNOCO card, and you have a full directional antenna that you can hold or mount on a small tripod. You take your gear to the lobby of the second floor, and you load up NetStumbler 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 entire second floor, waiting to 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 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 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 in the strong 128-bit mode, along with a complex 16-character passphrase for generating four keys. You will manually 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 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 utilize the full 128-bit key option, with the pre-shared WPA key option. The client computers 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 configure MAC address filtering. 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.

D- You determine that for the test network, you will run the network in infrastructure mode, using a SSID of FLOOR2. 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 the BSS, using the SSID of FLOOR2, and the access point will be configured with MAC address filtering of the test nodes. You will configure the access point to use EAP, specifically EAP-TLS. You will configure 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 theoffice, using the tool Ekahau. Working with this tool, you will map out and track the positioning of each wireless device once the network is active. 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.

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 access point. All test nodes will be configured to participate in the BSS, using the SSID of GlobalCorp, and the access point 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 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:

D

Question 9

Question Type: MultipleChoice

You got the router configured just as you wish, and it is time to get the team together for a meeting. You have the advantage of knowing several of these people for quite some time through your contracting, but this will be your first full meeting with them. The next day, you sit down with the CEO, HR Director, and other management people in MegaCorp. You wish for the meeting to be as short as possible, so in this initial meeting, you open with a short summary and project what you feel is a serious problem with the company. "Thanks for coming. I will try to keep this as brief as possible. As you all know, Red was let go under difficult circumstances, and for the last week I have been working non-stop to get the network and security under control here. Very good progress has been made, but we are missing a fundamental component. There is no security policy here at MegaCorp." To this, you see some heads nod in agreement, others have no reaction whatsoever, and a few people let go disappointing sighs. "I agree that we need a security policy," adds the HR Director, "as long as it doesn't become too restrictive." "Policies are only used to document the posture of the organization, and to provide some guidance in the direction of the network and, in this case, the security of the network." You add, "Without a written policy, how is any employee supposed to know what is acceptable, what is not acceptable, and so on." "Our employees have common sense, we do not want the company to become overly regulated," says a middle manager who you have not spoken with before. "Common sense is great, the more the employees have, and the easier it is to implement the policies. But, there is no guarantee for the human element. A simple review of what just took place with Red is a quick reminder of this." With that comment, the middle manager relaxed a bit, and hesitantly agreed. "So, what I would like to do is to lead the development of the policy here, and work with each of you to get it implemented. In the next few days, I will be requesting a bit of your time, so we can talk one on one about your needs and issues surrounding the policy." The next week, you meet with the management team, and you have a list of questions for them, designed to help you in drafting the security policy. You have decided to break up the creation of the policy into pieces, spending shorter blocks of time on the policy. This allows the management to be able to keep most of their days open for running the company. During the meeting, you focus solely on the

Acceptable Use statement for the users of the network. You ask the following questions to the group, and the consensus answer (after taking your suggestions into account) is listed after each question.

1.Are users allowed to share user accounts? No.

2.Are users allowed to install software without approval? No. Approval must come through you, or the current Chief Security Officer (CSO).

3.Are users allowed to copy software for archive or other purpose? No, archives can only be made by the network administration staff. 4.Are users allowed to read and\or copy files that they do not own, but have access to? Yes. 5.Are users allowed to make copies of any operating system files (such as the Windows directory or the SAM file)? No. 6.Are users allowed to modify files they do not own, but for which they have write abilities? Yes, if they have write abilities, they are allowed to modify the file. Using the provided information from the meeting, you draft the Acceptable Use Statement. The statement reads as follows:

This Acceptable Use Statement document covers MegaCorp, networks, computers, and computing resources. Network, computer, and computing resources are defined as physical personal computers, server systems, routers, switches, and network cabling. Also included in the definition are software (media) elements such as floppy disks, CD-ROMs (including writeable and re-writeable), DVD-ROMs, and tape backup systems. A user is defined as the individual account with authorization to access MegaCorp, resources. All users of the MegaCorp network are expected to conduct themselves in a respectful and legal manner. The MegaCorp, general computing systems are unclassified systems. As such, top-level secret information is not to be processed or stored on any general unclassified computer system. Individual users are responsible for the proper storage of their personal data on their workstations. For assistance on proper storage, users are instructed to contact the Security staff of MegaCorp. In the event that a user has identified a security breech, weakness, or system misuse in a MegaCorp, system, they are required to contact the on-duty Security staff immediately. Users are to use a completed MegaCorp-TPS Report for their notice to the Security staff. Initial contact with the Security staff about the incident might be conducted via email or telephone. Individual users are not granted access to systems and resources they have not been given explicit authority to access. In the event access to a resource is required, and access has not been granted, the user is to make a request to the on-duty Security staff. Individual users shall not make unauthorized copies of copy righted software, except as permitted

by law or by the owner of the copyright. Individual users are not permitted to make copies of system configuration files for their own, unauthorized personal use or to provide to other people or users for unauthorized uses. Individual users are not permitted to share, loan, or otherwise allow access to a MegaCorp resource via the user assigned account. Individual users are not permitted to engage in any online or offline activity with the intent or harass other users; degrade the performance of any MegaCorp, system or resource; impede the ability of an authorized user to access an authorized resource; or attempt to gain access to an unauthorized resource. Electronic mail resources are for authorized use only. Messages that might be deemed fraudulent, harassing, or obscene shall not be sent from, to, or stored on Mega Corp, systems.Individual users are not permitted to download, install, or run any unauthorized programs or utilities, including those which reveal weaknesses in the security of a system. This includes, but is not limited to network sniffing tools and password cracking utilities. Users who are found to be in violation of this policy will be reported to the on-duty Security staff and the MegaCorp CEO. The CEO will determine if the violation will result in the loss of MegaCorp, network privileges. In he event the violation warrants, the CEO may press civil or criminal charges against the user. I have read and understand the MegaCorp, Acceptable Use Statement, and agree to abide by it. With this information, and your knowledge of MegaCorp, choose the answer that will provide the best solution for implementing the Acceptable Use statement policy needs of MegaCorp:}

Options:

A- Once the meeting ends, you make the changes that were discussed during the meeting. They are not too extensive, but you make them and present the document to the team again on Friday. Now that you have made the changes, the policy is accepted, and the discussion moves towards getting every employee to sign and agree to the policy. 'Well, it's Friday afternoon. Everyone needs their paychecks today.' Comments the HR director. 'Good point, let just print out 100 of these, and tell everyone to sign them in order to get their check.' Agrees one of the' managers. After some discussion, it is agreed that this will be the fastest way to get all the employees to sign the policy document. The meeting wraps up around 2:00, and the printing and stapling of the policy documents ends around 4:00. Over the next hour, the HD director, with the help of the manager, hand our checks, making all the employees sign the document in order to get their check. You think to your self that the efficiency of a small operation like this is nice to see in action. You go to get your

check, sign your document, and are actually able to end your day at 5:00pm on a Friday.

B- You present the draft statement to the team at the next meeting. There is some discussion as to the wording in the clause regarding the internal TPS Report. Some in the group feel the TPS Report will be to tedious to use, others think with a distributed memo about the Report, everything will be fine. After further discussion all agree on the wording of the policy. The employees meet with the HR director over the next week, and are all presented with a copy of the policy and discuss how to it is to be implemented. There is some resistance, some of the employees are not happy about having a new procedure to follow. While walking back to your office, you see the CEO, and motion that you have a quick question, 'How does the new policy seem to be going with HR?' you ask. 'So far so good, there are a few folks not that happy, but I think wel be fine.' 'Ie got to get over there tomorrow to sign mine, when are you meeting with HR?' 'Me Ie got too much going on right now. I have to oversee everything; whatever happens and goes on here has to go through me anyway. I don't have time to bother with that myself, I just wanted to be sure we had something legally binding to protect us and to assist the employees.' 'Fair enough. Listen, I need to talk with you soon about our firewall situation,' you reply. 'OK, stop by anytime. You know my door is always open.' You walk away, and are pretty happy with how things are going here. You know you have more work to do, but so far your suggestions are being taken well and appreciated.

C- You present the current draft to the team at the next meeting. There is some discussion now on the language of the different clauses, and it seems that no one can agree on the points. What you thought was close to being done, now seems to be at risk of never getting done. As the meeting escalates, and opinions start to get louder, the CEO interrupts the group, 'Enough. We are a small group, we have enough in common, we know what we need out of this. We will bring in three contractors who specialize in policy writing. Wel give them our thoughts, they will work with our tireless Security Guru, and get this thing done.' You are not all that thrilled about three consultants coming down on your territory, but realize the frustration of the CEO. You agree, 'That fine by me. Il meet with them, and we will draft the document.' There is other business on the agenda for the meeting, but it is not related to you, so you excuse yourself and go back to your office. After working with the three consultants for a month, you have the document, approved by MegaCorp. You organize a company wide meeting, where the consultants describe the policy and what it is for to all the employees. The employees are told where they can find the policy to review for themselves, and after a question and answer session everyone gets back to their work.

D- You present the draft statement to the team at the next meeting. There is some discussion as to the wording in the clause regarding the internal TPS Report. Some in the group feel the TPS Report will be to tedious to use, others think with a distributed memo about the

Report, everything will be fine. After further discussion all agree on the wording of the policy. The team finishes the discussion, and the meeting ends with approval of the document. Once the document is approved, you move the discussion towards getting everyone in the company aware of and agreeing to it. 'I suggest that we tie it into our paychecks, and have the document go through HR.' 'We could do that, I guess. I can present the document to all the employees over the rest of the month.' the HR Director responds. Following that, the CEO brings up that there is going to be a company dinner next month, and that at the dinner the CEO will declare the policy in place, and that 'As all of us become comfortable with this, we all should appreciate this step forward for our company.' The next day, you post the policy on the company intranet site, so everyone has an electronic copy to go with their copy from the HR meeting. Once that is done, you move on to your next project.

E- After the review of the policy it is decided that some of the bullet points in the document need to be changed. You make the requested changes, and the team reviews the document once more. 'It all looks good to me now,' says a manager in the meeting. 'OK, how should we present this to the employees?' you ask. 'I could take a copy to each employee and discuss it with them,' offers the HR director. 'No, that would be too time-consuming. That not a good use of your time,' responds the CEO. 'We need to get this done, obviously. What is our most cost-effective way of doing this?' 'Well, I could post the policy on our intranet site, and we could have the employees go and download it themselves. During lunch, perhaps?' you suggest. 'That sounds good, let take that approach,' the CEO answers.' Later that day, you create a quick intranet site, called MegaCorp policy and documents. You draft a quick email, which will be sent to all the employees in the company:
'Dear _____, At MegaCorp we have just finished work on a security policy that will clearly define the use of the computers and other issues. This document will answer the questions that many of you have had recently on what you are allowed to do with the computer and when online. At your earliest convenience, please connect to the new site I have linked here, to download and read the new policy. Thanks and have a great day. -MegaCorp Security Staff.' You verify the site is working, send the email out to all the employees, and go home for the day.

Answer:

D

Question 10

Question Type: MultipleChoice

You finish the work you were doing in the morning, and head out to the monthly meeting. During this meeting, the Vice President of Strategic Partner Relations informs the group of some news, "we have decided that we need to implement a new web site that is for our strategic partners only. This site will be used for various purposes, but will primarily be used as a means of information exchange." "So, is this going to be a private site?" asks Blue. "Absolutely. We will not want any public users on this website. It's just for the people we identify in our Strategic Partner Program. I need those of you in security to be sure that this site is secure." "We can take care of that. How many people do you think will be accessing the site?" asks Blue. "Not too many, perhaps around fifty.""So, is it correct to assume that you know each of these fifty people?" "Yes, that is correct." "OK, well this should not be too hard. Wel get working on this right away." The meeting ends, and you and Blue chat more about the web site issue. "Well, we know that only around fifty people are going to access the, and we know who these fifty are. This should not cause too many problems," Blue says. "I agree. Do you think it will be all right to spend any money outside of the site itself?" you ask. "Since we are dealing with so few people, that shouldn be a problem. However, we cannot go overboard. Go ahead and write up a plan for this and get it back to me in a day or two." Based on your knowledge of Global Corp, choose the best solution to the web site security issue.}

Options:

A- You decide to use existing security technology of digital certificates and SSL to secure the site. You first install a new IIS server that will be the host of the web site. You then connect to the Globa lCorp CA for the executive building and request a new certificate for the web site. You then configure the web site to Require a Secure Channel (SSL) and install the certificate. One you install the new

certificate, you connect from the new server to the CA in each office where one or more of the fifty people that require access works. At that CA, you install the CA certificate, so that the new server will trust the certificates that each CA issues. Next, you return to the configuration of the new web site. To make the site more secure, you require client certificates, and enable mappings for each user account. You call each user and ensure that they have a certificate from their own CA, which the new server now trusts. You walk them through the process of connecting to the site, and verify that secure access to them has been granted.

B- You decide that you will use digital certificates to secure the website. You will first install a new private CA that the remote users can connect to and request their certificates. This CA will be protected with a very strong password. Each user will be given a user account to access the CA, also protected with a strong password. Next, you install the new private web server. You then connect to the new CA and make a request for a certificate for the web site. Once you receive the certificate, you configure the web site to use the certificate to Require a Secure Channel (SSL). You then select the option to require client certificates, and you enable mapping for each user account. Finally, you will call each person and instruct them on the process of connecting to the CA and requesting their certificate, which you will instruct them to store on their local machine. Once they have their certificate, you have them test access to the site, and when successful you move on to the next person.

C- You decide to use digital certificates on smart cards to secure the web site. You will first install a new IIS web server to host the site. You then connect to the CA_SERVER and request a new certificate for the server. The server certificate will be used for authentication, and you have the certificate issued and stored on a portable USB drive. You then configure a machine to function as the enrollment machine for smart cards. You are going to manage the smart cards yourself. At the machine that you are going to use for the smart cards, you first configure the system with an enrollment agent certificate from the CA_SERVER, and then you install the driver for the smart card reader. Once the driver is installed, you make certificate requests for each of the fifty users. You start with the first user, by logging in to the CA and selecting the option to Request A Certificate For A Smart Card On Behalf Of Another User Using The Smart Card Enrollment Station radio button. You then select the Smartcard User template, and enter the user name. When prompted, you put a blank smart card in the reader and press the Enroll button, followed by entering the default PIN. You then test access to the site from a remote machine using the smart card and PIN to be authenticated to the site. Once the test is complete, you write a short howto file and send it along with the smart card, smart card reader, and driver to each of the fifty users. You follow up with each user upon receipt to walk them through the configuration. D. You decide to use strong authentication via biometrics, specifically fingerprint scanning to secure

the web site. You will first install a new IIS web server to host the site. You then configure fifty user accounts for the remote users, and assign those accounts very strong passwords. You then ship one biometric mouse and software to each remote client. You call each user and walk them through the process of configuration of their equipment. First, you tell them to create a matching user account with the same user name and very strong password as you used on the IIS server. You then have them install the software, which you instruct them to configure so that the biometric will be linked to the user account. Once the software is installed, you instruct them to connect the mouse to their system and load the appropriate driver. With the driver installed, you tell them how to load the program and enroll their fingerprint. Once they have their fingerprint enrolled, and it is matched to their user account, you let them know that their side of the configuration is complete, and that you will call them shortly to finish the process. You return to the configuration of the IIS server. In the Security properties of the website, you select theAdvanced authentication tab. On the Advanced tab, you check the box for mapping user accounts to external biometric devices, and you check the box to allow the remote machine tocontrol the mapping. You finish the configuration by configuring the site to use 128 bit RSA to encrypt the data between the client and the server. With the server configuration done, you call the client back and have them log in using their biometric mouse. Once logged in, you instruct them to connect to the website and verify the secure site is running. E. You decide that you will use freely available PGP certificates to secure access to the website. You will first install a new IIS web server to hose the site. You then configure one user account, with a strong password. You map this account as the only account that has access to the website. You then log on locally, as this user account, to the server and create a public\private key pair. From that account you then send an outgoing email to all fifty users with the account private key. You finish the configuration of the website by making changes in the Security properties of the website. In the Security properties, you select the Advanced tab. On the Advanced tab, you check the box to map this account toa local digital certificate, and you select the new
certificate you just created. Next, you contact each remote user and instruct them to open the email from you. You have them store the key they receive in their personal certificate store. To verify the install is correct, you walk them through the process of viewing their certificates in the MMC. Once verified, you have the user connect to the website, and enter the location of their certificate when asked for authentication credentials.

Answer:

C