IEWB-SC-VOL2 Lab 2

Difficulty Rating (10 highest): 6

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/en/US/support/index.html.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information and routing protocols configuration.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the IPS sensor is either cisco/cisco or cisco/ciscoids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.INE.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
ASA Firewall	31
IOS Firewall	10
VPN	14
Identity Management	9
Ctrl/Mgmt Plane Security	7
IPS	11
Advanced Security	10
Network Attacks	8

GOOD LUCK!

1. ASA Firewall

1.1. ASA Addressing

- Configure the IP addresses for the inside and outside interfaces of ASA1 according to the diagram provided.
- Configure RackXASA1 as the hostname for the appliance.

2 Point

1.2. Firewall Contexts

- Activate multiple-contexts mode in ASA2.
- Create two security contexts named “ContextA” and “ContextB” as follows:
    - Allocate interfaces E0/0 and E0/1 to ContextA.
    - Allocate interfaces E0/0 and E0/2 to ContextB .
    - Configure interface names per the diagram provided
    - Set ContextA as the admin context.
- Users connecting to manage the firewall contexts should be unaware of real interface names and their physical characteristics.
- Configure RackXASA2 as ASA2’s hostname.

3 Points

1.3. Firewall Context Addressing

- Configure the IP addresses for the Inside and Outside interfaces of both security contexts in ASA2

2 Points

1.4. Firewall Context Routing

- Configure static routes for both firewall contexts of ASA2 to use SW1 as the default gateway.
- Configure two static routes on SW1 to provide connectivity to the VLAN133 and VLAN138 networks.
- Make sure the rest of the routing domain is able to reach the mentioned networks.

2 Points

1.5. Firewall Routing

- Configure RIPv2 between R2 and ASA1.
- ASA1 should send a default route alone to R2.
- Authenticate RIP updates between R2 and ASA1 using the password CISCO.
- This password should be sent in clear text.

3 Points

1.6. RIPv2

- Authenticate RIPv2 updates between ASA1 and R6 using a hash value that represents the password CISCO.

2 Points

1.7. NAT

- Configure ASA1 to translate any inside host's IP address to the outside interface's IP address.
- Translate all outbound ICMP packets to 132.X.69.222.

2 Points

1.8. BGP Authentication

- There is a BGP peering session configured between the Loopback0 interfaces of R2 and R6.
- Secure the BGP peering session between R2 and R6 using a hash value that represents the password value of CISCO.
- R6 should not be able to initiate the BGP session.

3 Points

1.9. NAT

- A web server has recently been installed in VLAN 29 with the IP address 132.X.29.100.
- The network administrator has requested that this web server be available to users outside of ASA1 via the IP address 132.X.69.100.
- Permit both HTTP and SSL connections to this server however connections should be denied during the weekends.

3 Points

1.10. NAT

- Any FTP connections that are attempted to this new web server's outside IP address should be redirected to the FTP server at 132.X.29.101.
- This FTP server is configured to listen for FTP connections on both ports 21 and 10021.
- To maintain compliance with the corporate security policy, ensure that ASA1 performs application inspection for the FTP connections made to both port 10021 along with port 21.

3 Points

1.11. Application Inspection

- A number of data servers have been recently installed behind the ASA2 in VLAN138.
- Users may access the servers by using FTP, HTTP and SMTP protocols.
- Configure an access control policy for the appropriate firewall context as follows:

    - Disallow uploads of files with extensions ".exe" and ".dll" via FTP
    - Use the local-domain "INE.com" for the SMTP server
    - Log any SMTP transactions violating this restriction
    - Drop any connections with e-mails being sent from the domain "cyberspam.org"
    - Reset TCP connections for any SMTP sessions that have probed for more than 10 incorrect e-mail recipients

- You policy should apply to all interfaces in the system, including any added in the future.

4 Points

1.12. NTP

- Configure ASA1 to synchronize its clock with BB1.
- Authenticate NTP updates using the MD5 hash and as password value of CISCO.

2 Points

2. IOS Firewall

2.1. CBAC

- After recent security issues internal to your network your manager has requested that R5's connection to BB2 be secured. After trying to figure out what your manager meant by "secured" you have decided to just implement CBAC on R1 using the following parameters:
    - Treat the link to BB2 as the outside interface and all other interfaces as inside.
    - Allow all TCP and UDP sessions initiated from the inside to return from the outside interface.
    - Permit outside hosts to connect via SSH to any device on the inside with the exception of outside hosts in the 192.10.X.0/24 network.
    - Permit all HTTP connections inbound.
    - Permit all necessary routing protocol traffic inbound.
    - Deny and log all other traffic.
- Do not apply an outbound access-list on R5's interface connected to BB2 to accomplish this task.
- Without any extra ACL statement, permit R5 to ping the outside destinations.

3 Points

2.2. CBAC Tuning

- On R1 configure CBAC to timeout idle TCP sessions after 30 minutes of inactivity.
- Inactive UDP sessions should be timed out after three minutes.
- DNS requests should be timed out after 10 seconds.

2 Points

2.3. NAT Virtual Interface

- Enable NAT on R4's Frame Relay and Serial interfaces. Do not designate the inside or outside interfaces explicitly.
- Use 132.X.255.0/24 for the address pool and translate the hosts on VLAN4 accessing the rest of the network using this pool.
- Advertise the pool subnet into OSPF, but do not use a static route for this.
- A web server with the IP address of 132.X.4.100 should be reachable via the IP address 132.X.255.100.
- The web server is running on the standard HTTP port of 80; SSL connections should also be permitted to this server.
- Any attempts to FTP to this server should be redirected to 132.X.4.101.

3 Points

2.4. Traffic Filtering

- Your manager has become concerned with packets coming from BB1 with spoofed source IP addresses.
- Configure R6 to drop packets without a verifiable source address received on its connection to BB1.
- Allow R6 to pings its own IP address on the Frame-Relay interface.

2 Point

3. VPN

3.1. IPsec VPN

- A new corporate policy has dictated that all traffic between VLAN 44 and VLAN 3 be encrypted.
- Do not use the **`crypto map`** command to accomplish this task.
- This encrypted traffic should use the following parameters:

    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: Default
    - ISAKMP Encryption: DES
    - ISAKMP SA Lifetime: 2400 seconds
    - ESP Encryption: DES
    - ESP Authentication: HMAC-MD5

- You are not allowed to use static routes for this task but you may use EIGRP AS# 34 for dynamic routing across the IPSec tunnel.

3 Points

3.2. VPN Client Support

- Configure ASA1 to support Cisco's VPN client on its outside interface using the following parameters:
    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: SHA
    - ISAKMP Encryption: 3DES
    - ESP Encryption: 3DES
    - ESP Authentication: HMAC-MD5
    - Address Pool: 10.255.255.1-10.255.255.254
    - Group Dame: CCIELAB
    - Group Password: CISCO
    - DNS Server: 132.X.29.50
    - Default Domain: INE.com
    - Idle Timeout: 1800 seconds
- Authenticate remote connections against the local database and create the username/password pair CCIEUSER/CISCO for this.
- ASA1 should authenticate this user against its local username/password database.

3 Points

3.3. IPSec VPN

- Encrypt all ICMP traffic between R1 and R6's Loopback0 interfaces using the following parameters:
    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: Default
    - ISAKMP Encryption: 3DES
    - ESP Encryption: 3DES
    - ESP Authentication: HMAC-SHA
- Configure the IPsec settings for minimum transport overhead.
- Do not modify any access-list in ASA1 to accomplish this task.

4 Points

3.4. GET VPN

- Allow R3 and R3 to exchange multicast traffic sourced off their Loopback0 interfaces to groups in range 239.0.0.0/8.
- The above-mentioned traffic should be protected using 3DES/MD5 for encryption and integrity validation.
- Use the scalable approach to encrypt multicast feeds.
- R2 should be responsible for the group key generation and use pre-shared key with the value of CISCO for ISAKMP authentication.

4 Points

4. Identity Management

4.1. TACACS+

- Against your recommendation the network administrator has decided that R5 should be managed via HTTP.
- Configure R5's HTTP management server to use TCP port 8080.
- Authenticate users via TACACS+ with the AAA server using the following parameters:
    - Authenticate the TACACS+ session with the AAA server using the password CISCO
    - Source the TACACS+ session off R5's Loopback0 interface
    - Create a user named R5WEB with the password CISCO in the AAA server for this authentication

3 Points

4.2. TACACS+

- Configure R3 to authenticate users telnetting into it with the following requirements:
    - Authenticate the TACACS+ session with the AAA server using the password CISCO
    - USER1 should be placed in privilege level 15 upon login
    - When USER1 successfully logs in execute the **`show users`** command automatically, but do not automatically disconnect them
    - USER2 should be placed in privilege level 2 and given access to all debug commands and the **`undebug all`** command.

- Create both users in the AAA server using the password value of CISCO for authentication.

3 Points

4.3. Authentication

- Authenticate users logging into R6 using local AAA authentication.
- Configure the usernames NOC and ADMIN both with passwords CISCO.
- Users that enter using the username NOC should be placed in privilege level 0.
- After entering the router they should be allowed access to privilege level 1 by using the password of LEVEL1.
- Users that login with the username of ADMIN should be automatically placed in privilege level 15.

3 Points

5. Control/Management Plane Security

5.1. Port Scanning

- In order to minimize the information revealed via port-scanning, configure R1 to drop any packets destined to closed TCP/UDP ports.
- Ensure the remote users may still connect to the port numbers 2001 and 7001.
- To minimize the impact of packets floods on R1's CPU, limit the aggregate rate of control-plane traffic to 10Kpps.
- Make sure the above policing does not affect BGP and OSPF routing protocols.

.

3 Points

5.2. SNMPv3

- Recently you realized that issues with the fan installed in R6 causes motherboard overheating under some circumstances.
- While waiting for the malfunctioning part replacement, configure R6 to inform the AAA server about any problems with environmental temperature via an SNMP message.
- Ensure the reliable delivery of the messages and encrypt them using 3DES cipher and the symmetric key value of CISCO.

.

4 Points

6. IPS

Read the access instructions for the IPS Sensor in the introduction for this lab prior to starting this section.

6.1. IPS Sensor Addressing

- Configure RackXIPS as the IPS's hostname.
- Configure the IP address for the command and control interface of the IPS according to the diagram provided.
- The IPS should use R1 as its default gateway.
- The login banner should say "Welcome to IPS".

2 Points

6.2. Traffic Monitoring

- An IPS sensor has been installed to monitor traffic as it enters your network via the Ethernet connection to ASA2.
- Allow management via telnet and HTTPS from IP addresses in the 10.0.0.0/24 and 132.1.170.0/24 networks.
- Configure SW2 to SPAN traffic sent/received on ASA2's interface E0/2 to the IPS sensor's sensing interface

3 Points

6.3. Network Access

- Configure the IPS to support blocking on both firewall contexts of ASA2.
- Enable the IPS sensor to access the firewall contexts using the username IPS and the password CISCO via SSH.
- The IPS sensor should never block the IP address of 131.X.138.100.

3 Points

6.4. Event Processing

- Configure the IPS to override the default action for targets having a Risk Rating value in the range of 50 - 100.
- With the action override the IPS should block the attacker.
- Configure the IPS such that any pings sent to servers in VLAN138 result in the action override.
- Do not modify any signature settings for this task.

3 Points

7. Advanced Security

7.1. Application Filtering

- Recently a new worm has been spreading through the Internet by exploiting a known vulnerability in Microsoft's Internet Information Server (IIS).
- Your manager is worried that the internal IIS servers will be affected by this worm and has asked that R1 be configured to prevent it from coming in their Internet connection to BB3.
- The only information you have about this worm is that it sends a HTTP GET request containing the strings "cmd.exe" or "root.exe".
- Configure R1 to drop any HTTP packets received across the link to VLAM 170 that contain URLs with these strings.

3 Points

7.2. Traffic Filtering

- Your NOC engineers have noticed an unusual flood of UDP packets destined for hosts in VLAN137 from sources located behind the R1 which appear to be at the SNMP service port.
- Configure SW1 to filter SNMP packets destined for VLAN137 that are sourced from any IP address other than IP addresses belonging to the 132.X.0.0/16 network.
- Be sure to take into consideration that there may be new ports added to this VLAN in near future.

3 Points

7.3. Secure Shell

- Your manager has determined that R1 and SW1 should only be managed via SSH as opposed to telnet.
- Configure SSH support on R1 and SW1.
- Authenticate remote users against the AAA server at 10.0.0.100.
- Create a user named SSH along with the password of CISCO in the AAA server.

2 Points

7.4. Router Hardening

- After returning from a network security class one of your network administrators has convinced your manager that R6 is open to many security vulnerabilities. To say the least your manager is not happy that these vulnerabilities have been left unchecked for so long. In order to appease him configure R6 to conform to the following security recommendations:

    - Disable CDP and Proxy-ARP on the Ethernet segment to ASA1
    - Disable BOOTP and DHCP server
    - Limit the rate of “ICMP unreachable” messages to 1 per second
    - A banner message should be displayed to all users that telnet into the router that states:

  Access to this device or the attached networks is prohibited without express written permission.

2 Points

8. Network Attacks

8.1. Flooding Attack Mitigation

- In response to recent ICMP DoS attacks on a web server located in VLAN 69 a new company policy dictates that ICMP echo traffic inbound on R6's connection to BB1 should be limited to 128kbps.
- In order to ensure that legitimate ICMP echo requests are not being dropped, allow the ICMP traffic to burst to 25% of the configured rate per second.
- Do not use MQC to accomplish this task.

2 Points

8.2. Layer 2 Filtering

- Your network administrator has voiced some concerns relating to the security of SW1's port Fa0/16 which is being used in the company's public conference room. In order to provide added security for this connection the network administrator has requested that only a device with the MAC address of 1234.5678.9abc be allowed to connect this port.
- If any other device attempts to connect to SW1's port Fa0/16 a log message should be generated and the port's state should be changed to error-disabled.

2 Points

8.3. Remotely Triggered Blackhole

- You network has been undergoing a flooding DoS attack sourced from the address range 115.0.0.0/8.
- To filter this traffic out at the edge of your network configure R2 as the trigger router and R6 as the edge router.
- Using BGP as the signaling protocol instruct the edge router to discard traffic sourced from network 115.0.0.0/8.
- Do not generate any ICMP messages when you drop packets.
- You are allowed to use static routes to Null0 to accomplish this.

4 Points