IEWB-SC-VOL2 Lab 3

Difficulty Rating (10 highest): 8

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 DVD format, and online at http://www.cisco.com/go/support

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.

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	20
IOS Firewall	14
VPN	13
Identity Management	9
Ctrl/Mgmt Plane Security	6
IPS	11
Advanced Security	19
Network Attacks	8

GOOD LUCK!

1. ASA Firewall

1.1. ASA1

- Configure ASA1 using the following guidelines:
    - Context Mode: Single Firewall Mode: Routed
    - Inside Security level: 99 Outside Security Level: 1
    - Inside interface name: “IN”,Outside interface name: “OUT”
    - Hostname: RackXASA1
- Configure interfaces E0/0 and E0/1 as a single logical interface. The Ethernet 0/1 interface should be the primary active interface. Configure a subinterface to pass traffic on VLAN 124 for the outside interface. Traffic for the inside interface should pass untagged. Configure switch interfaces as needed. For IP addressing, use a fourth octet value of 12 for the respective subnets.
- Configure the inside interface for OSPF area 51. For the connection to SW1, ASA1 should use plaintext authentication, using the password CISCO.
- ASA1 should drop traffic on the inside interface for which it does not have a valid route.
- The use of a default route is allowed to accomplish this task.

4 Points

1.2. ASA2

- Configure ASA2 using the following guidelines:
    - Context Mode: Single Firewall Mode: Routed
    - Inside Security level: 90 Outside Security Level: 10
    - Inside interface name: VLAN132 Outside interface name: VLAN135
    - Hostname: RackXASA2

- Configure interface E0/0 as the outside interface, and E0/1 as the inside interface. Do not configure any subinterfaces. For IP addressing, ASA2 should use a fourth octet value of 13.
- Configure both interfaces for RIPv2. ASA2 should send a default route to BB2 and a route for VLAN127. ASA2 should *not* send the default route to R5. RIP should use key# 1 with a value of CISCO, which should not be sent in plaintext.

4 Points

1.3. Address Translation

- Configure ASA1 to translate the address of the ACS server to 174.X.124.100 on the outside interface.
- To help prevent against a resource starvation attack, configure ASA1 to allow for a maximum of 250 TCP connections, 200 TCP half open connections, and 300 UDP connections for the ACS IP address. Do not use MPF configuration for this.
- Configure the ASA to permit traffic for RADIUS and TACACS+ protocols.
- Additionally, ensure R5 and R6 can peer iBGP between across the firewall using the translated IP address of 174.X.124.6 for R6's Loopback0.
- ACL entries for this task should not use any object groups or IP addresses.
- You may permit ICMP "ping" traffic across the firewall for connectivity testing.

3 Points

1.4. Object Groups

- Create an object group on ASA1 named HOSTS1.
- Put 10.0.0.100 and 10.0.0.101 in this object group.
- Create an additional object group on ASA1 named HOSTS2.
- Put 10.0.0.200 and 10.0.0.201 in this object group.
- Using a single access-list statement, deny ICMP echo requests on the inside interface from these hosts.

2 Points

1.5. SMTP Support

- In the near future a Microsoft Exchange server will be moved from VLAN 135 to VLAN 132 with the IP address of 192.10.x.200.
- The network administrator has requested ASA2 be configured to permit access from the outside to this server using IP address 174.x.135.200 on TCP ports 25 and 2525.
- Make sure ASA2 performs ESMTP application inspection on both ports.

2 Points

1.6. QoS

- A server with the IP address 192.10.X.75 in VLAN 132 runs FTP and HTTP applications.
- Configure ASA2 to permit HTTP and FTP (active mode) connections to this server.
- Users in VLAN 132 make voice over IP calls through ASA2; taking this in consideration configure QoS policy on the outside interface as follows:
    - Provide strict priority queue for VoIP data traffic.
    - Permit no more than 2Mbps of throughput for FTP and HTTP traffic, assuming FTP active mode for data transfers
    - Limit the aggregate bandwidth for the L2L VPN tunnel to 512Kbps.
    - Every remote VPN users should be limited to 64Kbps.

3 Points

1.7. System Monitoring

- Configure ASA2 for system messages logging using the host at IP address 10.0.0.100.
- Use the syslog facility LOCAL6 and log any message with a priority level of Informational and below.
- Use a reliable protocol for syslog messages transportation along with the default port value. Do not use any traffic encryption.
- The firewall should permit connections even if the syslog server is down.

2 Points

2. IOS Firewall

2.1. CBAC

- Using CBAC configure R5's interface FastEthernet 0/0 to allow inspection of telnet and SMTP sessions to a server located at 192.10.X.50. Audit-trails should also be enabled for these protocols.
- Telnet and SMTP traffic from this server should not be allowed inbound on the FastEthernet 0/0 interface, unless the session has been inspected.
- Configure R5 to log the CBAC information to the syslog server at 10.0.0.100.

2 Points

2.2. CBAC

- There is another server in VLAN 132 with IP address 192.10.X.60 which runs HTTP and FTP applications, however the services have TCP port numbers swapped: HTTP application listens on port 21 and FTP application listens on port 80.
- Configure CBAC to perform traffic inspection for these applications.
- Traffic from this server on these ports should not be allowed inbound on the FastEthernet0/0 interface, unless it has been inspected.

2 Points

2.3. Zone Firewall

- Configure R3 for Zone Based Firewall with the following guidelines:
- The Fa0/0 interface should be in security zone "A", Fa0/1 should be in security zone "B", and the Serial connection to R2 should be in zone "C".
- Allow ICMP traffic to pass freely, and other devices in your topology should be able to ping the interfaces of R3.
- Inspect TCP traffic from Zones A and B to zone C. Inspect UDP traffic from Zones A and B to zone C.
- You may allow additional inspections for other sections, as needed.

5 Points

2.4. Firewall Tuning

- Inspect Telnet traffic from Zone A to Zone C on ports 23 and 3020.
- Configure R2 to listen for telnet on TCP port 3020 for verification.
- Configure the firewall to log ICMP traffic.
- Enable audit trail for the telnet traffic on 3020, but not for the telnet traffic on port 23.

3 Points

2.5. URL Screening

- Configure R6 for HTTP URL filtering using a Websense server located at the IP address 10.0.0.100.
- HTTP access should be fully permitted in the event that the Websense server is down.
- Configure the domains “internetworkexpert.com” and “ine.com” as exempt from the access-control policy.
- Log URL information locally at the router.

2 Points

3. VPN

3.1. VPN Client

- The network administrator has requested that users in VLAN 53 be given access to a server located in VLAN 127. The traffic should be encrypted between the remote users and ASA1.
- The connections are to be protected by means of Cisco VPN Client.
- Configure ASA1 to support Cisco’s VPN client using the following parameters:
    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: SHA
    - ISAKMP Encryption: 3DES
    - ESP Encryption: 3DES
    - ESP Authentication: HMAC-SHA
    - Address pool: 10.105.105.1-10.105.105.50
    - Group Name: IPSECGROUP
    - Group Password: CISCO
    - Username: IPSECUSER
    - Password: CISCO

- Allow for split tunneling to destinations not in the 174.X.127.0/24 network.
- ASA1 should authenticate this user against the AAA server using RADIUS.

3 Points

3.2. IPsec VPN

- Create a LAN-to-LAN VPN Tunnel between VLAN 127 and 132 using the following parameters:
    - ISAKMP Authentication Method: RSA-SIG
    - ISAKMP Hash: SHA1
    - ISAKMP Encryption: 3DES
    - ISAKMP DH Group: Group 2
    - CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
    - ESP Encryption: AES-256
    - ESP Authentication: HMAC-MD5
- Configure ASA1 and ASA2 as tunnel endpoints for this task, but do not use the peer IP addresses for the tunnel-groups naming.

4 Points

3.3. DMVPN

- Create additional Loopback interfaces (Loopback 1) on R1, R4, and R5 using 10.255.Y.Y/24 for the addressing scheme.
- Source the tunnel off each router's respective Loopback 0 interface, using 10.255.255.Y/24 for addressing inside the tunnel.
- On R1, R4, and R5 enable OSPF area 0 for the Loopback 1 and GRE tunnel interfaces. Loopbacks should be advertised as /24's into OSPF.
- Encrypt the multipoint GRE tunnel on R1, R4 and R5 using the following parameters:
    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: MD5
    - ISAKMP Encryption: 3DES
    - ESP Encryption: AES-256
    - ESP Authentication: HMAC-SHA
- R1 should be the hub of the virtual network topology.

4 Points

3.4. DMVPN Features

- Encrypt the DMVPN traffic using IPSec cipher and hash AES256/SHA1 and ISAKMP policy with 3DES/MD5.
- The ISAKMP connections should be authenticated based on pre-shared keys using the key value of "CISCO".
- Configure R1, R4 and R5 so that the DMVPN spoke nodes do not need to query the hub's NHRP mapping table in order to discover the NBMA IP address of another spoke.

3 Points

4. Identity Management

4.1. Authentication

- The network administrator has requested that all HTTP sessions through ASA1 to the AAA server, be authenticated by ASA1 prior to being granted access.
- ASA1 should authenticate these users locally.
- The users will be entering username WEBUSER along with the password CISCO.
- Configure ASA1 to display the following banner to these users connecting via HTTP:

  Access to this server is for authorized personnel only

3 Points

4.2. Authentication & Authorization

- Recently a contractor made authorized configuration changes to R6. After the changes were completed the contractor made additional unauthorized configuration changes to R6 so that the contractor's computer would be accessible from the Internet. After recommending to your manager that this contractor be dismissed your manager has decided to just move this contractor's computer to the outside interface on ASA1 (VLAN 124) to help secure the internal network.
- To facilitate in this your manager has requested that R6 be configured to authenticate users logging in against the AAA server.
- The contractor will be logging into R6 using the IP 174.X.124.6 and username TROUBLEMAKER along with the password of CISCO.
- This user should be automatically placed into privilege level 15.

2 Points

4.3. Authentication

- Your manager has additionally requested that double authentication occur whenever the contractor attempts to telnet to R6.
- Configure ASA1 to authenticate the contractor locally prior to allowing the telnet session through to R6 using the username TROUBLEMAKER along with the password of CISCO.
- The contractor's IP address is 174.X.124.50.
- Do not require any other hosts in VLAN 124 to perform this authentication when telneting to R6.

2 Points

4.4. Accounting

- In order to help document the contractor's actions you have decided to configure accounting to the AAA server as follows:
    - Account when an EXEC process is created on R6.
    - Account for any level 15 commands executed on R6.
    - Account with the AAA server whenever the contractor makes a connection through ASA1.

2 Points

5. Control Plane / Management Security

5.1. SSH Administration

- Create two new local users on R4 for administration via SSH. Do not allow remote connections using telnet.
- A user named OPERATOR authenticated using the password of CISCO. Allow this user to configure any HTTP server settings. This user should not be able to configure interfaces.
- A user named ADMIN with the password CISCO who can perform any configuration.
- Console access should not be affected.
- Do not use change privilege levels for any commands to accomplish this task. Configuration for this task should be done entirely on R4.

4 Points

5.2. Routing Security

- SW1 has been pre-configured for an OSPF authentication key on the VLAN67 interface; however, this key is not currently being used, since authentication has not been enabled on the interface.
- Configure R6 to use the same key for the authentication, and enable plaintext authentication for the interface. On R6, the key should appear in the configuration in plain text (non-encrypted) form.

2 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 Management

- Configure the IPS for a hostname of RackXIPS. The IPS should use R3 as its gateway, and 174.X.38.10 as its IP address.
- Only allow management of the IPS sensor via telnet and HTTPS from the AAA server's IP address of 10.0.0.100.
- The AAA server should be able to telnet and browse (HTTPS) to 174.X.38.10 and reach the IPS sensor.
- Configure the IPS sensor to receive time via NTP from BB1.
- Authenticate the NTP updates using key 1 and the password CISCO.

4 Points

6.2. Inline Monitoring

- Configure SW2 to allow the IPS's sensing interface to monitor the traffic flowing through VLANs 102 and 106.
- Configure the IPS sensor to pair VLAN 102 and VLAN 106 for inline monitoring.

2 Points

6.3. IPS Management

- Due to a recent security vulnerability with certain IOS versions the network administrator has requested that a custom signature be created according to the following requirements:
    - ATOMIC.L3.IP engine: Signature ID 60001
    - IP Protocol Number: 77
    - Severity: High
- Use the default settings for alert summarization and signature fidelity rating.
- Log the attacker's traffic matching the custom signature.

2 Points

6.4. Custom Signature

- Configure the IPS sensor to block an attacker inline when IPS detects the substring "cmd.exe" in HTTP URLs.
- Do not use any STRING engine for that task.
- The new signature should have a high severity and medium fidelity rating.
- To make sure the IPS sensing engine is able to detect various IPS evasion techniques assume that the server may listen on ports 80 and 8080.
- Fire an event on every signature match.

3 Points

7. Advanced Security

7.1. Password Security

- Ensure that any passwords or authentication keys stored in R3 and R4's configuration are not readable in the **`show run`** output.

2 Points

7.2. Traffic Filtering

- An outside consultant recommended that R6's interface to the BB1 router be secured according to RFC 2827.
- Configure R6's interface connecting to the BB1 router to conform to this recommendation.

2 Points

7.3. Traffic Filtering

- Configure R6 to drop any traffic entering the Fa0/1 interface with Selective Directed Broadcast Options set.
- Traffic that does not have this should not be affected.

2 Points

7.4. Switch Filtering

- Configure SW2 to not send any ICMP unreachables out interface to any addresses in the RFC 1918 address space.

3 Points

7.5. NAT

- Configure NAT on R6 to translate any 150.X.0.0/16 IP addresses using a NAT pool consisting of 192.168.X.50 and 192.168.X.51 when sent across the Frame Relay cloud.
- Do not translate any other IP addresses.
- Ensure that pings sourced from an IP address in the network 150.X.0.0/16 can ping BB1.
- The use of one static route is permitted for this task.

3 Points

7.6. Worm Mitigation

- A new worm has been spreading through the Internet by exploiting a known vulnerability in Microsoft's Internet Information Server (IIS). You have been tasked with configuring R6 to prevent this worm from coming in from BB1.
- The information you have about this worm from a CERT Advisory states that the worm sends the string "root.exe" in the URL to the web server on TCP port 80.
- Configure R6 to drop any HTTP packets containing this string before forwarding the packet out either FastEthernet interface.

3 Points

7.7. DoS Prevention

- The network administrator is concerned about insecure telnet traffic on the serial connections of R4.
- Configure R4 to disallow any transit telnet traffic to exit via either of the serial interfaces. Do not use the command "match protocol" or configure any access lists to achieve this task.
- Telnet traffic on nonstandard ports should not be affected.

4 Points

8. Network Attacks

8.1. DoS Prevention

- The network administrator is concerned about possible SYN flood DoS attacks on servers in VLAN106 and VLAN102 and has requested that R6 be configured to help prevent attacks against these servers.
- Configure R6 to watch TCP sessions destined for servers in VLAN106 and VLAN102.
- R6 should reset the TCP session if the connection has not established within 15 seconds.
- R6 should start dropping partial connections once there are more than 1500 and should stop dropping them when the number of partial connections has fallen below 1200.
- The decision as to which partial connections are dropped should be random.

2 Points

8.2. TCP Normalization

- The server in VLAN132 with IP address 192.10.X.50 requires additional protection from possible network attacks.
- Configure ASA2 to stop forwarding fragmented packets on the outside interface.
- Limit number of TCP open/half-open sessions to the server to 2000 and 500 respectively.
- Configure ASA2 to normalize inbound TCP connections to the mentioned server as follows:

    - Ensure data integrity for TCP segments.
    - Make sure no data payload is carried in connection-establishment segments.
    - Explicitly permit TCP Echo and Echo Reply options.
    - Make sure that any reserved bits in TCP headers are cleared.

3 Points

8.3. Smurf Attack

- You network occasionally experiences Smurf attacks sourced from behind BB1. The ultimate targets are servers located in VLAN38.
- Since attacks are intermittent there is no actual reason to block all ICMP Echo-Reply traffic inbound on R6's link to BB1.
- Therefore, configure the IPS sensor to recognize this kind of attack and activate rate-limiting on R2 Frame-Relay interface in response.
- Limit offending traffic to 25% of the interface bandwidth.

3 Points