**EVALUACIÓN SUMATIVA - A**

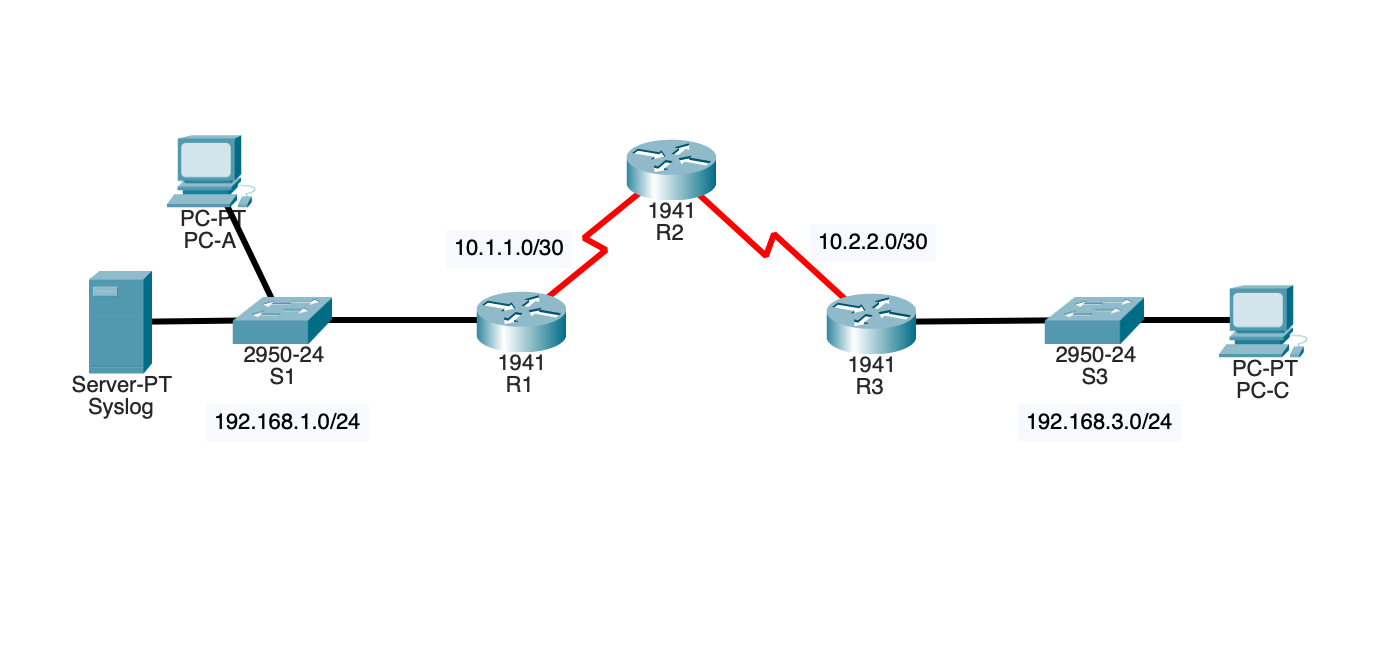
**Desafío de integración de habilidades**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Unidad 2:** Vulnerabilidades, procedimientos, acciones de mitigación y Controles de ISO 27001 | | | | | | |
| **Objetivos de la evaluación** | **Parte 1:**  En esta actividad del desafío, se debe terminar el esquema de direccionamiento, configurar el routing e implementar listas de control de acceso con nombre | | | | | |
| **Modalidad de trabajo** | Individual |  | Grupal | **X** | N° participantes: | 2-3 |
| **Formato de documento** | Packet Tracer | | | | | |

|  |
| --- |
| **Instructivo para la elaboración del trabajo** |

Configuración de un IPS

1. topología



1. Tabla de Direccionamiento

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara | Puerta de enlace predeterminada | Cambiar puerto |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N / A | T1 F0/5 |
| S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N / A | N / A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N / A | N / A |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N / A | N / A |
| R3 | G0/1 | 192.168.3.1 | 255.255.255.0 | N / A | T3 F0/5 |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N / A | N / A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | T1 F0/6 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | T3 F0/18 |

1. Objetivos

Parte 1: Configuraciones básicos

* Configurar hostname, dirección IP en interfaces, y contraseñas.
* Configurar ruta estática.

Parte 2: Usar CLI para configurar en IOS un IPOS

* Configurar IOS IPS usando CLI.
* modificar firmas IPS.
* Examinar los resultados de configuración IPS.
* Verificar la funcionalidad IPS.
* Registrar mensajes IPS en un servidor syslog

Parte 3: Simular un ataque

* Usar una herramienta de escaneo para simular un ataque .

1. Antecedentes / Escenario
2. En esta actividad, se configurará IPS en IOS Cisco, la que forma parte del conjunto de funciones de Cisco IOS Firewall. El IPS examina ciertos patrones de ataque, alertando o mitigando esos ataques, cuando ocurren esos patrones. El IPS por sí solo no es suficiente para convertir un router en un firewall de Internet seguro, pero cuando se agrega a otras características de seguridad, puede ser una defensa efectiva.
3. Se configurará un IPS utilizando el CLIde Cisco IOS y luego se probará la funcionalidad de IPS. Para ello, se cargará el paquete de firma IPS desde un servidor TFTP y configurará la clave criptográfica pública mediante Cisco IOS.
4. Nota: Los comandos y la salida del router en esta práctica de laboratorio provienen de un router Cisco 1941 con Cisco IOS versión 15.4(3)M2. Se pueden utilizar otros routers y versiones de Cisco IOS. Los comandos disponibles y la salida producida están determinados por el modelo de router y la versión de Cisco IOS utilizada. Por lo tanto, pueden variar de lo que se muestra en esta actividad.
5. Nota: Asegúrese de que los routers y conmutadores se hayan borrado y no tengan configuraciones de inicio.
6. configurar los ajustes básicos del router

En la Parte 1, se configurará la topología de la red y configurará los ajustes básicos, como nombres de host, direcciones IP de interfaz, enrutamiento estático, acceso a dispositivos y contraseñas.

Nota: Realice los pasos enumerados en la Parte 1 en los tres routers. Solo R1 se muestra a continuación.

* + 1. Verificar la conexión de la red como se muestra en la topología

Conecte los dispositivos, como se muestra en el diagrama de topología, y cablee según sea necesario.

* + 1. Configure los ajustes básicos para cada router .
       1. Configure los nombres de host, como se muestra en la topología.
       2. Configure las direcciones IP de cada interfaz, como se muestra en la tabla de direcciones IP .
       3. Configure el clock rate en la interfaz serial con cable DCE conectado.

R1(config)# **interface S0/0/0**

R1(config-if)# **clock rate 64000**

* + - 1. Deshabilitar la búsqueda de DNS para evitar que el router intente traducir comandos ingresados ​​incorrectamente.

R1(config)# no ip domain-lookup

* + 1. Configurar el enrutamiento estático en los routers .
       1. Configure una ruta estática por defecto IPv4 de siguiente salto, desde R1 a R2 y desde R3 a R2.
       2. Configure una ruta estática IPv4 desde R2 a la LAN de R1 (192.168.1.0) y desde R2 a la LAN de R3 (192.168.3.0) usando el siguiente salto apropiado.
    2. Configurar los PC.

Configure IP estática, máscara de subred, y default gateway de PC-A y PC-C, como se indica en la tabla de direccionamiento.

* + 1. verificar Conectividad .
       1. Realice ping desde R1 a R3.

Si los pings no tienen éxito, resuelva los problemas de las configuraciones básicas del dispositivo antes de continuar .

* + - 1. Realice ping desde PC-A en la LAN de R1 a PC-C en la LAN de R3.

Si los pings no tienen éxito, resuelva los problemas de las configuraciones básicas del dispositivo antes de continuar.

**Nota** : Si se puede hacer ping desde la PC-A a la PC-C, se ha demostrado que el protocolo de enrutamiento estático está configurado y funciona correctamente. Si no puede hacer ping, pero las interfaces del dispositivo están activas y las direcciones IP son correctas, use los comandos **show run** y **show ip route** para identificar problemas relacionados con el protocolo de enrutamiento.

* + 1. Configure una cuenta de usuario, contraseñas cifradas y claves criptográficas para SSH.

**Note** : Las contraseñas en esta tarea se fortalecieron en un mínimo de 10 caracteres, pero son relativamente simples para el beneficio de realizar la práctica de laboratorio. Se recomiendan contraseñas más complejas en una red de producción .

* + - 1. Configure una longitud mínima de contraseña mediante el comando de **contraseñas de seguridad** para establecer una longitud mínima de contraseña de 10 caracteres.

R1(config)# **security passwords min-length 10**

* + - 1. Configurar un nombre de dominio.

R1(config)# **ip domain-name ccnasecurity.com**

* + - 1. Configurar claves criptográficas para SSH

R1 (config) # **crypto key generate rsa general-keys modulus 1024**

* + - 1. Configure una cuenta de usuario admin01 usando **scrypt de tipo algoritmo** para el cifrado y una contraseña de cisco12345.

R1 (config) # **username admin01 algorithm-type scrypt secret cisco12345**

* + - 1. Configure la consola de línea 0 para usar la base de datos de usuarios local para los inicios de sesión. Para mayor seguridad, el **exec-timeout** El comando hace que la línea se desconecte después de cinco minutos de inactividad. El comando de **registro síncrono** evita que los mensajes de la consola interrumpan la entrada del comando.

**Nota** : para evitar inicios de sesión repetitivos durante esta práctica de laboratorio, el comando **exec-timeout** se puede establecer en **0 0** , lo que evita que caduque. Sin embargo, esto no se considera una buena práctica de seguridad.

R1(config)# **line console 0**

R1(config-line)# **login local**

R1(config-line)# **exec-timeout 5 0**

* + - 1. R1(config-line)# **logging synchronous** Configure la línea auxiliar 0 para usar la base de datos de usuarios locales para los inicios de sesión .

R1(config)# **line aux 0**

R1(config-line)# **login local**

R1(config-line)# **exec-timeout 5 0**

* + - 1. Configurar linea vty 0 4 para usar la base de datos de usuarios locales para inicios de sesión y restringir el acceso solo a conexiones SSH.

R1(config)# **line vty 0 4**

R1(config-line)# **login local**

R1(config-line)# **transport input ssh**

R1(config-line)# **exec-timeout 5 0**

* + - 1. Configure la contraseña de habilitación con un cifrado fuerte.

R1(config)# **enable algorithm-type scrypt secret class12345**

* + 1. Guarde las configuraciones básicas para los tres routers.

Guarde la configuración en ejecución en la configuración de inicio desde el indicador del modo EXEC privilegiado.

R1# **copy running-config startup-config**

1. Configuración de IPS mediante el CLIde Cisco IOS

En la Parte 2 de esta práctica de laboratorio, usted configure IPS en el R1 mediante el CLIde Cisco IOS. Luego revisa y prueba la configuración resultante.

* 1. Verificar el acceso a la LAN de R1 desde R2

En esta tarea, verificará que sin IPS configurado, el R2 externo puede hacer ping a la interfaz S0/0/0 del R1 y a la PC-A en la LAN interna del R1.

* + 1. Haga ping de R2 a R1.

Desde R2, haga ping a la interfaz S0/0/0 de R1 en la dirección IP 10.1.1.1.

R2# **ping 10.1.1.1**

Si los ping no tienen éxito, resuelva los problemas de las configuraciones básicas del dispositivo antes de continuar.

* + 1. Haga ping desde el R2 a la PC-A en la LAN del R1.

Desde el R2, haga ping a la PC-A en la LAN del R1 en la dirección IP 192.168.1.3.

R2# **ping 192.168.1.3**

Si los ping no tienen éxito, resuelva los problemas de las configuraciones básicas del dispositivo antes de continuar.

* + 1. Muestre la configuración en ejecución del R1 antes de configurar IPS.

Emita el comando **show run** para revisar la configuración básica actual en el R1.

¿Hay algún comando de seguridad relacionado con IPS?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 2: Prepare el router y el servidor TFTP**

* + 1. Verifique la disponibilidad de los archivos IPS de Cisco IOS .

Para configurar Cisco IOS IPS 5.x, el archivo de paquete de firma IOS IPS y el archivo de clave criptográfica pública deben estar disponibles en la PC-A. Consulte con su instructor si estos archivos no están en la PC. Estos archivos se pueden descargar de www. cisco.com con una cuenta de usuario válida que tenga la autorización adecuada.

* + - 1. Verifique que el archivo IOS-S *xxx* -CLI.pkg esté en una carpeta TFTP. Este es el paquete de la firma. El *xxx* es el número de versión y varía según el archivo que se descargó.
      2. Verifique que el archivo realm-cisco.pub.key.txt esté disponible y observe su ubicación en la PC-A. Esta es la clave criptográfica pública utilizada por IOS IPS.
    1. Verifique o cree el directorio IPS en la memoria flash del router en el R1.
       1. En este paso, verificará la existencia o creará un directorio en la memoria flash del router donde se almacenarán las configuraciones y los archivos de firma requeridos.

**Nota** : Como alternativa, puede usar una unidad flash USB conectada al puerto USB del router para almacenar los archivos de firma y las configuraciones. La unidad flash USB debe permanecer conectada al puerto USB del router si se utiliza como ubicación del directorio de configuración de IOS IPS. IOS IPS también admite cualquier sistema de archivos Cisco IOS como su ubicación de configuración con acceso de escritura adecuado.

* + - 1. Desde el CLIde R1, muestre el contenido de la memoria flash usando el comando **show flash y busque el ipsdir**directorio.

R1 # **show flash**

* + - 1. Si el directorio **ipsdir** no aparece en la lista, créelo en modo EXEC privilegiado .

R1# **mkdir ipsdir**

Create directory filename [ipsdir]? <**Enter**>

Created dir flash:ipsdir

* + - 1. Si el directorio ya existe, se muestra el siguiente mensaje:

%Error Creating dir flash:ipsdir (Can't create a file that exists)

Utilice el comando de eliminación para borrar el contenido del **directorio ipsdir** .

R1# **delete flash:ipsdir/\***

Delete filename [/ipsdir/\*]?

Delete flash:/ipsdir/R1-sigdef-default.xml? [confirm]

Delete flash:/ipsdir/R1-sigdef-delta.xml? [confirm]

Delete flash:/ipsdir/R1-sigdef-typedef.xml? [confirm]

Delete flash:/ipsdir/R1-sigdef-category.xml? [confirm]

Delete flash:/ipsdir/R1-seap-delta.xml? [confirm]

Delete flash:/ipsdir/R1-seap-typedef.xml? [confirm]

**Nota** : Utilice este comando con precaución. Si no hay archivos en el directorio **ipsdir** , aparece el siguiente mensaje:

R1# **delete flash:ipsdir/\***

Delete filename [/ipsdir/\*]?

No such file

* + - 1. Desde el CLIde R1, verifique que el directorio esté presente mediante el comando **dir flash:** o **dir flash:ipsdir** .

R1# **dir flash:**

Directory of flash:/

1 -rw- 75551300 Feb 16 2015 01:53:10 +00:00 c1900-univeralk9-mz.SPA.154-3.M2.bin

2 drw- 0 Mar 8 2015 12:38:14 +00:00 ipsdir

or

R1# dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory

**Nota** : el directorio existe, pero actualmente no hay archivos en él.

* 1. Configurar la clave criptográfica IPS

La clave criptográfica verifica la firma digital del archivo de firma maestra (sigdef-default.xml). Los contenidos están firmados por una clave privada de Cisco para garantizar la autenticidad e integridad en cada lanzamiento.

* + 1. Copie y pegue el archivo de clave criptográfica en R1.

En el modo de configuración global, seleccione y copie el archivo de clave criptográfica llamado **realm-cisco.pub.key.txt** .

crypto key pubkey-chain rsa

named-key realm-cisco.pub signature

key-string

30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001

quit

* + 1. Aplique el contenido del archivo de texto al router.

En el indicador del modo EXEC privilegiado de R1, ingrese al modo de configuración global mediante el comando **configure terminal.**

* + - 1. Pegue el contenido de la clave criptográfica copiada en el indicador del modo de configuración global.

R1(config)#

R1(config)# **crypto key pubkey-chain rsa**

R1(config-pubkey-chain)# **named-key realm-cisco.pub signature**

R1(config-pubkey-key)# **key-string**

Enter a public key as a hexidecimal number ....

R1(config-pubkey)#**$2A864886 F70D0101 01050003 82010F00 3082010A 02820101**

R1(config-pubkey)#**$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16**

R1(config-pubkey)#**$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128**

R1(config-pubkey)#**$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E**

R1(config-pubkey)#**$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35**

R1(config-pubkey)#**$994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85**

R1(config-pubkey)#**$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36**

R1(config-pubkey)#**$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE**

R1(config-pubkey)#**$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3**

R1(config-pubkey)# **F3020301 0001**

R1(config-pubkey)# **quit**

R1(config-pubkey-key)#

* + - 1. Salga del modo de configuración global y emita el comando **show run** para confirmar que la clave criptográfica está configurada.
  1. Configurar IPS
     1. Cree una regla IPS.
        1. En R1, cree un nombre de regla IPS usando el nombre de **ip ips name**comando en el modo de configuración global. Asigne el nombre **iosips a** la regla de IPS . Esto se usará más adelante en una interfaz para habilitar IPS.

R1(config)# **ip ips name iosips**

* + - 1. Puede especificar una lista de control de acceso (ACL) opcional extendida o estándar para filtrar el tráfico que será analizado por este nombre de regla. Todo el tráfico permitido por la ACL está sujeto a inspección por parte del IPS. El tráfico denegado por la ACL no es inspeccionado por el IPS.
      2. Para ver las opciones disponibles para especificar una ACL con el nombre de la regla, utilice el comando **ip ips name** y la función de ayuda de el CLI( **?** ).

R1(config)# **ip ips name ips list ?**

<1-199> Numbered access list

WORD Named access list

* + 1. Configure la ubicación de almacenamiento de la firma IPS en la memoria flash del router.

Los archivos IPS se almacenarán en el directorio **ipsdir** que se creó en la Tarea 2, Paso 2. Configure la ubicación con el comando **ip ips config location .**

R1(config)# **ip ips config location flash:ipsdir**

* + 1. Habilite la notificación de eventos IPS SDEE .

El servidor Cisco Security Device Event Exchange (SDEE) es un protocolo de acceso a objetos simple (SOAP), formato de alerta IDS y especificación de protocolo de transporte. SDEE reemplaza a Cisco RDEP.

Para usar SDEE, el servidor HTTP debe estar habilitado con el comando **ip http server .** Si el servidor HTTP no está habilitado, el router no puede responder a los clientes SDEE porque no puede ver las solicitudes. La notificación SDEE está deshabilitada de forma predeterminada y debe habilitarse explícitamente.

R1 (config) # **ip http server**

Para habilitar SDEE, use el siguiente comando:

R1 (configuración) # **ip ips notify sdee**

* + 1. Habilite la compatibilidad con syslog de IPS.

IOS IPS también admite el uso de syslog para enviar notificaciones de eventos. SDEE y syslog se pueden usar de forma independiente o habilitarse al mismo tiempo para enviar notificaciones de eventos IOS IPS. La notificación de Syslog está habilitada de forma predeterminada.

* + - 1. Si el registro de la consola está habilitado, se muestran los mensajes de syslog de IPS. Habilite syslog si no está habilitado.

R1(config)# **ip ips notify log**

* + - 1. Utilice el comando **show clock para verificar la hora y la fecha actuales del router.** Use el comando **clock set** en el modo EXEC privilegiado para restablecer el reloj si es necesario. El siguiente ejemplo muestra cómo configurar el reloj.

R1# **clock set 01:20:00 20 march 2022**

* + - 1. Verifique que el servicio de marca de tiempo para el registro esté habilitado en el router mediante el comando **show run .** Habilite el servicio de marca de tiempo si no está habilitado.

R1 (config) # **service timestamps log datetime msec**

* + - 1. Para enviar mensajes de registro al servidor syslog en la PC-A, use el siguiente comando:

R1 (config) # **logging 192.168.1.3**

* + - 1. Para ver el tipo y el nivel de registro habilitado en el R1, use el **comando show logging** dominio.

R1# **show logging**

**Nota** : Verifique que tenga conectividad entre el R1 y la PC-A haciendo ping desde la PC-A a la dirección IP de la interfaz Fa0/1 del R1 **192.168.1.1** . Si no tiene éxito, resuelva los problemas según sea necesario antes de continuar.

El siguiente paso describe cómo descargar uno de los servidores syslog gratuitos si uno no está disponible en la PC-A.

* 1. Probar la regla IPS y modificar una firma

Puede trabajar con firmas de muchas maneras. Pueden ser retirados y no retirados, habilitados y deshabilitados, y sus características y acciones pueden cambiarse. En esta tarea, primero prueba el comportamiento predeterminado de IOS IPS haciendo ping desde el exterior.

* + 1. Haga ping desde R2 a la interfaz serial 0/0/0 de R1.

Desde el CLIen el R2, haga ping al R1 S0/0/0 en la dirección IP **10.1.1.1** . Los ping son exitosos porque se retiró la firma ICMP Echo Request 2004:0.

* + 1. Haga ping desde R2 a PC-A.

Desde el CLIen el R2, haga ping a la PC-A en la dirección IP **192.168.1.3** . Estos ping también son exitosos debido a la firma retirada. Este es el comportamiento predeterminado de las firmas IPS.

R2# **ping 192.168.1.3**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

* + 1. Modificar la firma.

Puede utilizar el CLIde Cisco IOS para cambiar el estado de la firma y las acciones para una firma o un grupo de firmas en función de las categorías de firma.

El siguiente ejemplo muestra cómo anular la retirada de la firma de la solicitud de eco, habilitarla, cambiar la acción de la firma a alerta y descartar y restablecer la firma 2004 con un ID de subsig de 0.

R1(config)# **ip ips signature-definition**

R1(config-sigdef)# **signature 2004 0**

R1(config-sigdef-sig)#**status**

R1(config-sigdef-sig-status)# **retired false**

R1(config-sigdef-sig-status)# **enabled true**

R1(config-sigdef-sig-status)# **engine**

R1(config-sigdef-sig-engine)# **event-action produce-alert**

R1(config-sigdef-sig-engine)# **event-action deny-packet-inline**

R1(config-sigdef-sig-engine)# **event-action reset-tcp-connection**

R1(config-sigdef-sig-engine)# **exit**

R1(config-sigdef-sig)# **exit**

R1(config-sigdef)# **exit**

Do you want to accept these changes? [confirm] <**Enter**>

Mar 8 05:37:45.775: %IPS-6-ENGINE\_BUILDS\_STARTED: 05:37:45 UTC Mar 8 2015

Mar 8 05:37:46.099: %IPS-6-ENGINE\_BUILDING: atomic-ip - 539 signatures - 1 of 13 engines

R1(config)#

Mar 8 05:37:51.219: %IPS-6-ENGINE\_READY: atomic-ip - build time 5120 ms - packets for this engine will be scanned

Mar 8 05:37:51.427: %IPS-6-ALL\_ENGINE\_BUILDS\_COMPLETE: elapsed time 5652 ms

|  |
| --- |
| **Instrucciones:** |
| * Es importante cumplir con la formalidad de redacción del documento. * El trabajo es grupal * Una vez finalizado el trabajo, se debe subir a la plataforma, en formato Packet Tracer. |
| **Estructura y formato general:** |
| Para desarrollar esta actividad se ha dispuesto de un archivo con la topología ya pre configurada, para facilitar tu trabajo. Para tener éxito en esta actividad, es importante que completes cada una de sus partes. |

**Pauta de evaluación:**

En base al resultado del desarrollo de la actividad en el simulador Packet Tracer, se convierte a nota el porcentaje según la siguiente escala:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Porcentaje | Nota |  | Porcentaje | Nota |  | Porcentaje | Nota |  | Porcentaje | Nota |
| 0 | 1 |  | 26 | 2,3 |  | 51 | 3,6 |  | 76 | 5,2 |
| 1 | 1,1 |  | 27 | 2,4 |  | 52 | 3,6 |  | 77 | 5,3 |
| 2 | 1,1 |  | 28 | 2,4 |  | 53 | 3,7 |  | 78 | 5,4 |
| 3 | 1,2 |  | 29 | 2,5 |  | 54 | 3,7 |  | 79 | 5,4 |
| 4 | 1,2 |  | 30 | 2,5 |  | 55 | 3,8 |  | 80 | 5,5 |
| 5 | 1,3 |  | 31 | 2,6 |  | 56 | 3,8 |  | 81 | 5,6 |
| 6 | 1,3 |  | 32 | 2,6 |  | 57 | 3,9 |  | 82 | 5,7 |
| 7 | 1,4 |  | 33 | 2,7 |  | 58 | 3,9 |  | 83 | 5,7 |
| 8 | 1,4 |  | 34 | 2,7 |  | 59 | 4 |  | 84 | 5,8 |
| 9 | 1,5 |  | 35 | 2,8 |  | 60 | 4 |  | 85 | 5,9 |
| 10 | 1,5 |  | 36 | 2,8 |  | 61 | 4,1 |  | 86 | 6 |
| 11 | 1,6 |  | 37 | 2,9 |  | 62 | 4,2 |  | 87 | 6 |
| 12 | 1,6 |  | 38 | 2,9 |  | 63 | 4,2 |  | 88 | 6,1 |
| 13 | 1,7 |  | 39 | 3 |  | 64 | 4,3 |  | 89 | 6,2 |
| 14 | 1,7 |  | 40 | 3 |  | 65 | 4,4 |  | 90 | 6,3 |
| 15 | 1,8 |  | 41 | 3,1 |  | 66 | 4,5 |  | 91 | 6,3 |
| 16 | 1,8 |  | 42 | 3,1 |  | 67 | 4,5 |  | 92 | 6,4 |
| 17 | 1,9 |  | 43 | 3,2 |  | 68 | 4,6 |  | 93 | 6,5 |
| 18 | 1,9 |  | 44 | 3,2 |  | 69 | 4,7 |  | 94 | 6,6 |
| 19 | 2 |  | 45 | 3,3 |  | 70 | 4,8 |  | 95 | 6,6 |
| 20 | 2 |  | 46 | 3,3 |  | 71 | 4,8 |  | 96 | 6,7 |
| 21 | 2,1 |  | 47 | 3,4 |  | 72 | 4,9 |  | 97 | 6,8 |
| 22 | 2,1 |  | 48 | 3,4 |  | 73 | 5 |  | 98 | 6,9 |
| 23 | 2,2 |  | 49 | 3,5 |  | 74 | 5,1 |  | 99 | 6,9 |
| 24 | 2,2 |  | 50 | 3,5 |  | 75 | 5,1 |  | 100 | 7 |
| 25 | 2,3 |  |  |  |  |  |  |  |  |  |