Ciberseguridad

Nivel Intermedio – Integrador

Misión 1

CASO 1: situación de intento de intrusión es detectado por el IPS

Situación: Un intento de intrusión es detectado por el IPS al intentar explotar una vulnerabilidad conocida en uno de los servidores web en la DMZ.

Acciones Tomadas:

1. Bloqueo Inmediato: El IPS bloquea automáticamente el tráfico malicioso y envía una alerta al equipo de seguridad.
2. Investigación: El equipo de seguridad revisa los logs del SIEM, identificando la fuente del ataque y verificando si hubo algún impacto en otros sistemas.
3. Actualización de Políticas: Basado en la información obtenida, se ajustan las reglas del cortafuegos y las configuraciones del IPS para prevenir futuros intentos similares.
4. Parches y Actualizaciones: Se aplican parches de seguridad al servidor web afectado para corregir la vulnerabilidad explotada.

PoC (Proof of Concept)

Para la implementación de un cortafuegos, la configuración de una DMZ, la segmentación de red mediante VLANs, la implementación de VPN y el uso de un SIEM. Utilizaremos un cortafuegos basado en iptables en Linux, configuraciones de Cisco IOS para VLANs y VPN, y una herramienta SIEM como Splunk.

Configuración de un Cortafuegos con iptables

a. Filtrado de Paquetes Básico

```
# Limpiar reglas existentes
sudo iptables -F
# Políticas predeterminadas
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT

# Permitir tráfico en la interfaz de loopback
```

```
sudo iptables -A INPUT -i lo -j ACCEPT

# Permitir tráfico SSH desde una IP específica
sudo iptables -A INPUT -p tcp -s 192.168.1.100 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# Permitir tráfico HTTP/HTTPS
sudo iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

# Loguear y descartar todo el tráfico restante
sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: "
sudo iptables -A INPUT -j DROP
```

b. Configuración de DMZ

--

```
# Asumimos que la interfaz eth1 está conectada a la DMZ

# Permitir tráfico HTTP/HTTPS hacia la DMZ

sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i eth1 -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i eth1 -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT


# Permitir respuestas DNS de la DMZ

sudo iptables -A FORWARD -i eth1 -o eth0 -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
```

Configuración de VLANs en Cisco IOS

```
# Entrar en modo de configuración global
enable
configure terminal
# Crear VLANs
vlan 10
name Development
vlan 20
name Management
vlan 30
name Users
# Asignar puertos a VLANs
interface range gigabitEthernet 0/1 - 10
switchport mode access
switchport access vlan 10
interface range gigabitEthernet 0/11 - 20
switchport mode access
switchport access vlan 20
interface range gigabitEthernet 0/21 - 30
switchport mode access
switchport access vlan 30
```

Configurar Trunking para el enlace entre switches

interface gigabitEthernet 0/24

switchport trunk encapsulation dot1q

switchport mode trunk

Configuración de VPN en Cisco IOS

Entrar en modo de configuración global

enable

configure terminal

Configuración de ISAKMP

crypto isakmp policy 10

encryption aes

hash sha256

authentication pre-share

group 14

lifetime 86400

```
crypto isakmp key myPreSharedKey address 0.0.0.0

# Configuración de IPsec
crypto ipsec transform-set myTransformSet esp-aes esp-sha-hmac

crypto map myCryptoMap 10 ipsec-isakmp
set peer 198.51.100.1
set transform-set myTransformSet
match address 101

# Aplicar el mapa crypto a la interfaz
interface gigabitEthernet 0/0
crypto map myCryptoMap

# Crear lista de acceso para tráfico de VPN
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

Configuración de SIEM con Splunk

a. Instalación y Configuración Básica

```
# Descargar e instalar Splunk
wget -O splunk-8.2.6-linux-2.6-amd64.deb 'https://www.splunk.com/page/download_track?file=8.2.6/linux/splunk-8.2.6-linux-2.6-amd64.deb'
sudo dpkg -i splunk-8.2.6-linux-2.6-amd64.deb

# Iniciar Splunk
sudo /opt/splunk/bin/splunk start --accept-license

# Crear un usuario admin
sudo /opt/splunk/bin/splunk enable boot-start
sudo /opt/splunk/bin/splunk add user admin -role admin -password MyStrongPassword

# Añadir datos de logs de iptables
sudo /opt/splunk/bin/splunk add monitor /var/log/syslog -sourcetype linux_syslog
```

b. Configuración de Alertas en Splunk

Acceder a la interfaz web de Splunk en http://localhost:8000

Navegar a "Search & Reporting" y crear una nueva búsqueda:

index=main sourcetype=linux_syslog "IPTables-Dropped"

Guardar la búsqueda como una alerta:

- Guardar > Guardar como alerta

- Configurar la alerta para que se ejecute en tiempo real

- Establecer condiciones de disparo (por ejemplo, más de 10 eventos en 1 minuto)

- Configurar acciones de alerta, como enviar un correo electrónico a admin@example.com