Universidad Francisco de Vitoria
UFV Madrid

Incidentes de ciberseguridad

Contención de un ataque

Nombre:	Fecha:	Edición:	Firma:
Gonzalo Pascual Romero	21/03/2023	1.0	Firmado por ***0960** GONZALO PASCUAL el día 21/03/2024 con un certificado emitido por AC CAMERFIRMA FOR NATURAL

Índice

1. Medidas de contención: Bloqueo de IPs

Tras activar el plan de respuesta, es crucial implementar medidas de contención para frenar el incidente, como evitar la propagación de infecciones o detener la exfiltración de datos. Estas acciones temporales deben ser proporcionales y ágiles para no interrumpir el funcionamiento básico de la organización. La experiencia del equipo es esencial, y se deben obtener autorizaciones antes de tomar medidas drásticas, documentando cada paso dado. Una de las medidas utilizadas es la configuración de los firewalls para bloquear el acceso desde direcciones IP maliciosas o puertos utilizados en ataques, así como inspeccionar el tráfico en busca de contenido dañino.

2. Caso de prueba:

En el caso práctico voy a hacer una configuración del firewall creando reglas de bloqueo para peticiones de entrada y de salida, para realizar la comprobación voy a tener una segunda máquina desde la que lanzaré pruebas para comprobar el sistema de contención

La máquina donde voy a realizar las reglas de bloqueo es un ordenador Ubuntu con la IP:

192.168.22.14

```
root@Ubuntu:/home/ubuntu# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.14  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::971e:d5a7:3134:dbea  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ae:fa:7d  txqueuelen 1000  (Ethernet)
```

Y la máquina desde donde voy a realizar las pruebas es una Kali con la IP:

192.168.22.6

```
┌──(kali㉿Gonzalo)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.6  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::7ef2:bb03:5f73:3135  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3a:f8:e9  txqueuelen 1000  (Ethernet)
```

Para hacer los bloqueos a las IPs voy a descargar Iptables que es una herramienta de firewall para Linux que permite controlar el tráfico de red entrante y saliente

```
root@Ubuntu:/home/ubuntu# apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.7-1ubuntu5.1).
iptables set to manually installed.
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libllvm13
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
```

Bloque de entrada:

Primero comprobamos que se pueda hacer una solicitud desde la Kali a la Ubuntu. Para probarlo hago un nmap a la ip y me dice que el host esta activo y también le hago un ping y lo responde perfectamente por lo que vemos claramente que las peticiones están entrando

```
┌──(kali㉿Gonzalo)-[~]
└─$ nmap 192.168.22.14
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-20 17:38 EDT
Nmap scan report for 192.168.22.14
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.22.14 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(kali㉿Gonzalo)-[~]
└─$ ping 192.168.22.14
PING 192.168.22.14 (192.168.22.14) 56(84) bytes of data.
64 bytes from 192.168.22.14: icmp_seq=1 ttl=64 time=0.525 ms
64 bytes from 192.168.22.14: icmp_seq=2 ttl=64 time=1.53 ms
64 bytes from 192.168.22.14: icmp_seq=3 ttl=64 time=0.744 ms
^Z
zsh: suspended  ping 192.168.22.14
```

Ahora voy a realizar una regla para bloquear la IP de la máquina Kali

```
root@Ubuntu:/home/ubuntu# iptables -A INPUT -s 192.168.22.6 -j DROP
root@Ubuntu:/home/ubuntu#
```

Una vez con la regla aplicada volvemos a hacer un nmap y esta vez dice que el host parece que este caído y el ping no lo consigue hacer y nos lo bloquea

```
┌──(kali㉿Gonzalo)-[~]
└─$ nmap 192.168.22.14
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-20 17:43 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds

┌──(kali㉿Gonzalo)-[~]
└─$ ping 192.168.22.14
PING 192.168.22.14 (192.168.22.14) 56(84) bytes of data.

^Z
zsh: suspended  ping 192.168.22.14
```

Bloque de salida:

En el caso anterior hemos bloqueado las solicitudes entrantes de la máquina, pero no las salientes, vamos a comprobar que se pueda hacer un ping desde la máquina Ubuntu a la Kali

```
root@Ubuntu:/home/ubuntu# ping 192.168.22.14
PING 192.168.22.14 (192.168.22.14) 56(84) bytes of data.
64 bytes from 192.168.22.14: icmp_seq=1 ttl=64 time=0.123 ms
64 bytes from 192.168.22.14: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.22.14: icmp_seq=3 ttl=64 time=0.047 ms
```

Por lo que ahora tenemos que hacer una regla que también bloquee las peticiones salientes de la máquina Ubuntu

```
root@Ubuntu:/home/ubuntu# iptables -A OUTPUT -s 192.168.22.14 -j DROP
```

Y ahora con la nueva norma aplicada volvemos a realizar el ping para comprobar que este no llega

```
root@Ubuntu:/home/ubuntu# ping 192.168.22.14
PING 192.168.22.14 (192.168.22.14) 56(84) bytes of data.
```

Más reglas:

A parte de esas se pueden aplicar muchas más reglas para bloquear o redirigir paquetes según criterios como direcciones IP, puertos y protocolos

Podemos permitir tráfico de entrada en un puerto específico

```
root@Ubuntu:/home/ubuntu# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Podemos bloquear todo el tráfico de entrada y salida, excepto el tráfico relacionado y establecido

```
root@Ubuntu:/home/ubuntu# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@Ubuntu:/home/ubuntu# iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@Ubuntu:/home/ubuntu# iptables -A INPUT -j DROP
root@Ubuntu:/home/ubuntu# iptables -A OUTPUT -j DROP
```

Y también podemos bloquear todas las peticiones entrantes y salientes de cualquier IP

```
root@Ubuntu:/home/ubuntu# iptables -P INPUT DROP
root@Ubuntu:/home/ubuntu# iptables -P OUTPUT DROP
```