FOIRE AUX QUESTIONS ASA/IPS : Comment l'IPS affiche-t-il de vraies adresses IP non traduites dans les journaux d'événements ?

Contenu

Introduction

Ce document explique comment le Système de protection contre les intrusions Cisco (IPS) affiche de vrais logs non traduits d'addressess IP en cas, bien que l'appliance de sécurité adaptable (ASA) envoie le trafic à l'IPS après qu'elle exécute le Traduction d'adresses de réseau (NAT).

Informations générales

Topologie

- L'adresse IP privée du serveur : 192.168.1.10
- L'adresse IP publique du serveur (Natted) : 203.0.113.2
- L'adresse IP de l'attaquant : 203.0.113.10

Comment l'IPS affiche-t-il de vraies adresses IP non traduites dans les journaux d'événements ?

Explication

Quand l'ASA envoie un paquet à l'IPS, elle encapsule ce paquet dans une en-tête de Protocol du fond de panier de **Module de services de** Cisco **ASA/Security (SSM)**. Cette en-tête contient un champ qui représente la vraie adresse IP de l'utilisateur intérieur derrière l'ASA.

Ces logs affichent un attaquant qui envoie des paquets de **Protocole ICMP (Internet Control Message Protocol) à l'**adresse IP publique du serveur, 203.0.113.2. Le paquet capturé sur l'IPS prouve que l'ASA donne un coup de volée les paquets à l'IPS après avoir exécuté NAT.

```
IPS# packet display PortChannel0/0
```

```
Warning: This command will cause significant performance degradation
tcpdump: WARNING: po0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on po0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:40:06.239024 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239117 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239903 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
03:40:06.239946 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
```

Voici les logins IPS d'événement pour des paquets de demandes d'ICMP de l'attaquant.

```
IPS# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: po0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on po0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:40:06.239024 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239117 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239903 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
03:40:06.239946 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
```

Voici les logins IPS d'événement pour la réponse d'ICMP du serveur intérieur.

```
IPS# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: po0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on po0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:40:06.239024 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239117 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239903 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
03:40:06.239946 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
```

Voici les captures collectées sur le plan de données ASA.

```
IPS# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: po0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on po0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
03:40:06.239024 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239117 IP 203.0.113.10 > 192.168.1.10: ICMP echo request, id 512, seq
31232, length 40
03:40:06.239903 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
03:40:06.239946 IP 203.0.113.2 > 203.0.113.10: ICMP echo reply, id 512, seq
31232, length 40
```

Captures décodées de **plan de données ASA**.

Informations connexes

- Guide de configuration CLI de capteur de Système de protection contre les intrusions Cisco IPS 7.1
- Le paquet traversent le Pare-feu de Cisco ASA
- Support et documentation techniques - Cisco Systems