

AUDIT DISCOVERY

Powered by :
Forgelab



SOMMAIRE

1. Wazuh Audit 1 Techniques MITRE &ttack

Wazuh Audit, 29/11/24

Mitre ID	Name	Phase	State
T1590	Netstat Execution - Basique		Discovery
T1589	Whoami Commande - Basique		Discovery
T1589	Whoami Bypass - Espaces		Discovery
T1589	Whoami Bypass - Copie du binaire		Discovery
T1590	Netstat Execution Bypass - Copie du binaire		Discovery
T1590	Netstat Execution Bypass - Fichiers systèmes		Discovery
T1590	Netstat Execution Bypass - Espaces		Discovery

2. Details

A. T1590 - Netstat Execution - Basique

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations réseau de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.



Commandes RedTeam :

```
alex@server:~$ netstat -ntlp
(No info could be read for "-p": geteuid()=1000 but you should
be root.)
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address
tcp	0	0	0.0.0.0:443	0.0.0.0:*
LISTEN	-			
tcp	0	0	0.0.0.0:32768	0.0.0.0:*
LISTEN	-			
tcp	0	0	0.0.0.0:25	0.0.0.0:*
LISTEN	-			
tcp	0	0	0.0.0.0:1515	0.0.0.0:*
LISTEN	-			
tcp	0	0	0.0.0.0:1514	0.0.0.0:*
LISTEN	-			
tcp	0	0	127.0.0.53:53	0.0.0.0:*
LISTEN	-			
tcp	0	0	0.0.0.0:2222	0.0.0.0:*
LISTEN	-			

alex@server:~\$

 Réaction et détection BlueTeam :

Détecté par le SIEM (rule.id : 100001)

B. T1589 - Whoami Commande - Basique

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations d'identité de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

 **Commandes RedTeam :**

```
alex@server:~$ whoami
alex
alex@server:~$
```

Réaction et détection BlueTeam :

Détecter par le SIEM (rule.id : 100002)

C. T1589 - Whoami Bypass - Espaces

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations d'identité de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

Commandes RedTeam :

```
alex@server:~$ whoami
alex
alex@server:~$
```

Réaction et détection BlueTeam :

Détecté par le SIEM (rule.id : 100002) - elle est détectée car elle reconnait l'exécutable whoami.

D. T1589 - Whoami Bypass - Copie du binaire

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations d'identité de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

Commandes RedTeam :

```
alex@server:~$ cp $(which whoami) /tmp/mytool
alex@server:~$ /tmp/mytool -ntlp
alex@server:~$ whoami
alex
alex@server:~$
```

Réaction et détection BlueTeam :

Le fait de copier le binaire dans un autres fichier, puis d'exécuter ce dernier permet de contourner la règle (remonté dans les logs auditd en Low).

Solution :

- Monitorer la modification / création de fichier dans des répertoires spécifique.

Action a réaliser :

<https://documentation.wazuh.com/current/user-manual/capabilities/command-monitoring/use-cases/check-if-the-output-changed.html>

E. T1590 - Netstat Execution Bypass - Copie du binaire

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations réseau de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

Commandes RedTeam :

```
alex@server:~$ cp $(which netstat) /tmp/mytool

alex@server:~$ /tmp/mytool -ntlp
(No info could be read for "-p": geteuid()=1000 but you should
be root.)
```

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
      PID/Program name
tcp        0      0 0.0.0.0:443            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32768          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1515           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1514           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2222           0.0.0.0:*               LISTEN
```

Réaction et détection BlueTeam :

Le fait de copier le binaire dans un autres fichier, puis d'exécuter ce dernier permet de contourner la règle (remonté dans les logs auditd en Low).

Solution :

- Monitorer la modification / création de fichier dans des répertoires spécifique.

Action a réaliser :

<https://documentation.wazuh.com/current/user-manual/capabilities/command-monitoring/use-cases/check-if-the-output-changed.html>

F. T1590 - Netstat Execution Bypass - Fichiers systèmes

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations réseau de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

Commandes RedTeam :

```
alex@server:~$ cat /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr
tm->when retransmt   uid  timeout inode
   0: 00000000:01BB 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 11561 1 0000000000000000
100 0 0 10 0
   1: 00000000:8000 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 325057 1 0000000000000000
100 0 0 10 0
   2: 00000000:0019 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 12673 1 0000000000000000
100 0 0 10 0
   3: 00000000:05EB 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 3275217 1 0000000000000000
100 0 0 10 0
   4: 00000000:05EA 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 3274525 1 0000000000000000
100 0 0 10 0
   5: 3500007F:0035 00000000:0000 0A 00000000:00000000
00:00000000 00000000    992          0 9359 1 0000000000000000
100 0 0 10 5
   6: 00000000:08AE 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 8966 1 0000000000000000
100 0 0 10 0
   7: 00000000:0BB9 00000000:0000 0A 00000000:00000000
00:00000000 00000000      0          0 122

alex@server:~$ cat /proc/net/udp
  sl  local_address rem_address   st tx_queue rx_queue tr
tm->when retransmt   uid  timeout inode ref pointer drops
 388: 3600007F:0035 00000000:0000 07 00000000:00000000
00:00000000 00000000    992          0 9360 2 0000000000000000 0
 388: 3500007F:0035 00000000:0000 07 00000000:00000000
00:00000000 00000000    992          0 9358 2 0000000000000000 0
 3228: 00000000:EB4D 00000000:0000 07 00000000:00000000
00:00000000 00000000    112          0 7910 2 0000000000000000 0
 5688: 00000000:14E9 00000000:0000 07 00000000:00000000
00:00000000 00000000    112          0 7908 2 0000000000000000 0
alex@server:~$
```


Réaction et détection BlueTeam :

Cette commande n'a pas été détecté car elle interroge directement les fichiers système sans exécuter un binaire externe.

Solution :

- Monitorer la lecture de répertoires sensibles.

G. T1590 - Netstat Execution Bypass - Espaces

Le but de ce premier audit est de tester le déploiement et le contournement de règles de la tactique Reconnaissance (pour la technique "Récupération d'informations réseau de la victime compromise").

L'environnement est un ubuntu server (24.04.1 LTS) avec un agent Wazuh installé.

Commandes RedTeam :

```
alex@server:~$ netstat -ntlp
(No info could be read for "-p": geteuid()=1000 but you should
be root.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
0
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN
0
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
0
tcp        0      0 0.0.0.0:1515            0.0.0.0:*               LISTEN
0
tcp        0      0 0.0.0.0:1514            0.0.0.0:*               LISTEN
0
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
0
tcp        0      0 0.0.0.0:2222           0.0.0.0:*               LISTEN
0
```

3. Bilan de l'audit

Les bons points

- **Détection efficace des commandes standards :**
 - Les commandes classiques comme netstat et whoami ont été correctement détectées par Wazuh.
 - Les tentatives de contournement par ajout d'espaces ont également été interceptées.

Les points à améliorer

- **Contournements réussis :**
 - **Copie de binaires :** Copier un binaire (ex. whoami ou netstat) sous un autre nom permet de contourner les règles existantes.
 - **Accès direct aux fichiers système :** La lecture directe de fichiers critiques comme /proc/net/tcp n'est pas détectée.

Améliorations proposées

1. **Surveillance des fichiers sensibles :**
 - Mettre en place des règles pour surveiller les modifications ou créations de fichiers dans des répertoires critiques (ex. /tmp, /proc).
2. **Détection des copies de binaires :**
 - Activer le monitoring des commandes copiées et les exécutions dans des répertoires non standard.
3. **Renforcement des règles :**
 - Améliorer les signatures de détection pour inclure des variations de commandes avec espaces et chemins non standards à l'aide de regex.

En mettant en œuvre ces améliorations, la couverture de détection pour les activités de reconnaissance et de contournement sera significativement renforcée.