Nation-State Cyber Attack Response

Executive Summary

November 2022

David Sánchez

1. THREAT DETECTION

1.1. Malware detection

Antivirus scanning was performed with ClamAV in order to detect malware files that the attacker could have brought into the server. Initial results showed 3 files identified as malware (Annex 1, 1.1).

1.2. Malicious files

Another suspicious file was found on the server as shown below. This file is a script that downloads and tries to execute processes (Annex 1, 1.2). In order to avoid similar files that cannot be detected with ClamAV by default, a Yara Rule was created (Annex 1, 1.3).

2. THREAT MITIGATION

2.1. HIDS & Suspicious IPs

The OSSEC tool (Host based Intrusion Detection System) was used in order to detect suspicious logs from the server related to a brute force attack that led to an unauthorized access event (Annex 2, 2.1). Using this information, it was possible to recognize the IP address related to the attack (Annex 2, 2.2). SSH configurations were made in order to prevent the IP address from connecting through SSH again (Annex 2, 2.3).

2.2. Backdoor Detection

Logs at OSSEC showed the creation of a new user after a successful login as “root” user (Annex 2, 2.4).

As the attacker had access as “root” user, new processes could be launched as “root” user. Amongst those running processes, one could not be identified. It is thought that this is a backdoor for the attacker in order to regain access to the server (Annex 2, 2.5).

In order to remove the persistence created by the attacker, the suspicious user and process were removed from the server (Annex 2, 2.6). Furthermore, configurations to avoid access as “root” user through SSH was made and it is no longer possible (Annex 2, 2.7).

3. SYSTEM HARDENING FOR ENHANCED SECURITY

3.1. Vulnerability Scanning

The OpenVAS scan was used in order to identify vulnerabilities in the server. Several vulnerabilities were found at the server. Results for this scanning process can be found at Annex 3 (3.1).

3.2. Securing Apache Server

Metadata from the Apache Server was hidden in order to mitigate the risk of a successful exploit (Annex 3, 3.2). Furthermore, a new user and user group with low privileges was created specifically for the Apache service (Annex 3, 3.3).

4. RECOMMENDATIONS

4.1. Standard nomenclature for usernames

Develop standard names for allowed users and delete those that do not follow the policy.

Example of user another suspicious user was found at the server:

```
$ cat /etc/passwd
# voldemort:x:0:0::/home/voldemort:
```

4.2. Password manager and MFA authentication policy

Stablish a policy related to the usage of a password manager for sensitive credential storage. Thus, enforce Multi-factor Authentication (MFA) for organization's users and apply its configuration on SSH servers.

4.3. IPs Whitelist

Create a whitelist of IP address that are allowed to connect remotely through SSH.

4.4. Firewall policy

Develop policy related to firewalls that help mitigate attacks.

4.5. Isolate service

Configuration with regard to jailing the service in order to avoid isolate potential attacks.

ANNEX

1. MALWARE DETECTION

1.1. ClamAV scan result

```
# /home/ubuntu/Downloads/ft32: Unix.Malware.Agent-6774375-0 FOUND
# /home/ubuntu/Downloads/ft64: Unix.Malware.Agent-6774336-0 FOUND
# /home/ubuntu/Downloads/wipefs: Unix.Tool.Miner-6443173-0 FOUND
```

1.2. Malicious files: suspicious URL

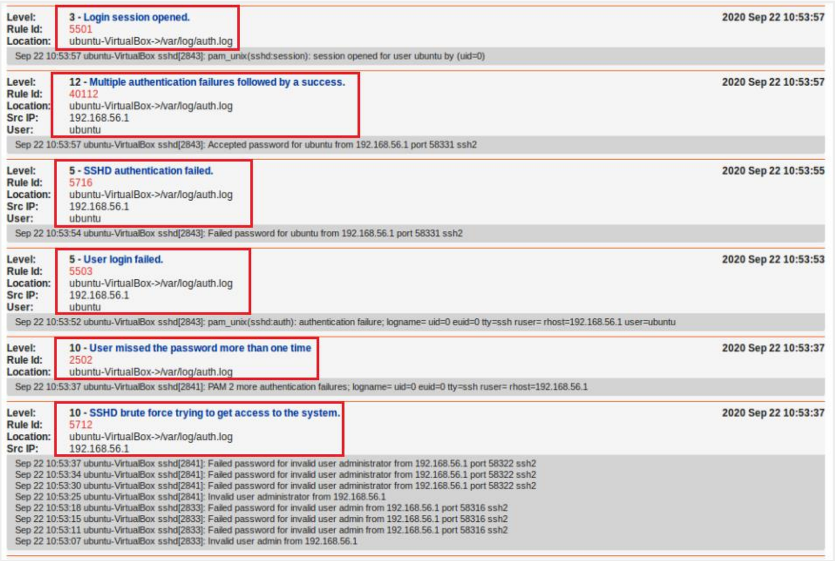
```
$ cat SSH-One
# hfs_m=http://darkl0rd.com:7758/SSH-T
# hfs_s=http://darkl0rd.com:7758/SSH-One
```

1.3. Malicious files: Yara Rule for suspicious URL

```
Note
A Yara Rule was created in order to identify files that match any name that
contains "darkl0rd". The rule "unknown_threat.yara" is defined as follows:
---------------------------------------------------------------------------
rule unknown_threat {
    meta:
        Author = "@ubuntu"
        Description = "rule detects the presence of any files coming from
'darkl0rd'"
    strings:
        $url1 = /.*(darkl0rd).*/
    condition:
        any of them
}
---------------------------------------------------------------------------
```

2. THREAT MITIGATION

2.1. Logs from OSSEC: successful login after brute force attack



```
Level:     3 - Login session opened.                                  2020 Sep 22 10:53:57
Rule Id:   5501
Location:  ubuntu-VirtualBox->/var/log/auth.log
  Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)

Level:     12 - Multiple authentication failures followed by a success.  2020 Sep 22 10:53:57
Rule Id:   40112
Location:  ubuntu-VirtualBox->/var/log/auth.log
Src IP:    192.168.56.1
User:      ubuntu
  Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2

Level:     5 - SSHD authentication failed.                            2020 Sep 22 10:53:55
Rule Id:   5716
Location:  ubuntu-VirtualBox->/var/log/auth.log
Src IP:    192.168.56.1
User:      ubuntu
  Sep 22 10:53:54 ubuntu-VirtualBox sshd[2843]: Failed password for ubuntu from 192.168.56.1 port 58331 ssh2

Level:     5 - User login failed.                                     2020 Sep 22 10:53:53
Rule Id:   5503
Location:  ubuntu-VirtualBox->/var/log/auth.log
Src IP:    192.168.56.1
User:      ubuntu
  Sep 22 10:53:52 ubuntu-VirtualBox sshd[2843]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1 user=ubuntu

Level:     10 - User missed the password more than one time           2020 Sep 22 10:53:37
Rule Id:   2502
Location:  ubuntu-VirtualBox->/var/log/auth.log
  Sep 22 10:53:37 ubuntu-VirtualBox sshd[2841]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1

Level:     10 - SSHD brute force trying to get access to the system.  2020 Sep 22 10:53:37
Rule Id:   5712
Location:  ubuntu-VirtualBox->/var/log/auth.log
Src IP:    192.168.56.1
  Sep 22 10:53:37 ubuntu-VirtualBox sshd[2841]: Failed password for invalid user administrator from 192.168.56.1 port 58322 ssh2
  Sep 22 10:53:34 ubuntu-VirtualBox sshd[2841]: Failed password for invalid user administrator from 192.168.56.1 port 58322 ssh2
  Sep 22 10:53:30 ubuntu-VirtualBox sshd[2841]: Failed password for invalid user administrator from 192.168.56.1 port 58322 ssh2
  Sep 22 10:53:25 ubuntu-VirtualBox sshd[2841]: Invalid user administrator from 192.168.56.1
  Sep 22 10:53:18 ubuntu-VirtualBox sshd[2833]: Failed password for invalid user admin from 192.168.56.1 port 58316 ssh2
  Sep 22 10:53:15 ubuntu-VirtualBox sshd[2833]: Failed password for invalid user admin from 192.168.56.1 port 58316 ssh2
  Sep 22 10:53:11 ubuntu-VirtualBox sshd[2833]: Failed password for invalid user admin from 192.168.56.1 port 58316 ssh2
  Sep 22 10:53:07 ubuntu-VirtualBox sshd[2833]: Invalid user admin from 192.168.56.1
```

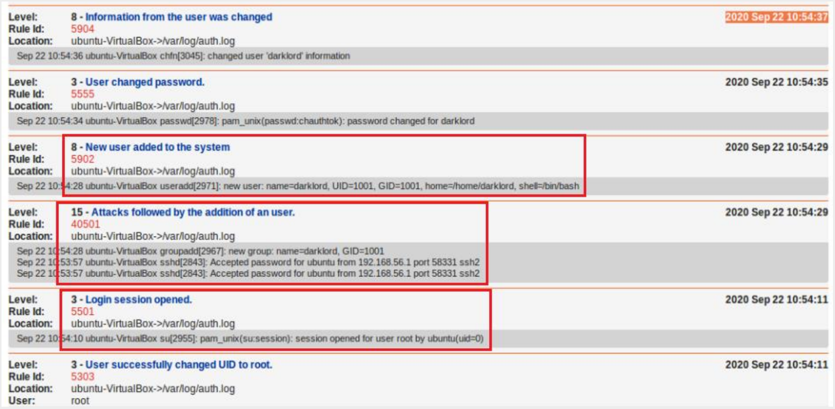
2.2. IP address found at attack

```
Note
The suspicious login events related to the attack can be found since "2020
Sep 22 10:50:00". The log related to the successful login is found at the
image below.
The suspicious IP address associated with the attack was identified:
192.168.56.1
```

2.3. SSH rule for blocking IP address SSH connections

```
Note
A IPtables rule was made in order to make sure that SSH remote connection
requests coming from the suspicious IP are blocked. Detail of the rule is
found below.
-----------------------------------------------------------------------
$ SUSP_IP="192.168.56.1"
$ iptables -I INPUT -s $SUSP_IP -j DROP
-----------------------------------------------------------------------
```

2.4. Creation of new user after successful "root" user login



```
Level:     8 - Information from the user was changed                2020 Sep 22 10:54:37
Rule Id:   5904
Location:  ubuntu-VirtualBox->/var/log/auth.log
 Sep 22 10:54:36 ubuntu-VirtualBox chfn[3045]: changed user 'darklord' information

Level:     3 - User changed password.                               2020 Sep 22 10:54:35
Rule Id:   5555
Location:  ubuntu-VirtualBox->/var/log/auth.log
 Sep 22 10:54:34 ubuntu-VirtualBox passwd[2978]: pam_unix(passwd:chauthtok): password changed for darklord

Level:     8 - New user added to the system                         2020 Sep 22 10:54:29
Rule Id:   5902
Location:  ubuntu-VirtualBox->/var/log/auth.log
 Sep 22 10:54:28 ubuntu-VirtualBox useradd[2971]: new user: name=darklord, UID=1001, GID=1001, home=/home/darklord, shell=/bin/bash

Level:     15 - Attacks followed by the addition of an user.        2020 Sep 22 10:54:29
Rule Id:   40501
Location:  ubuntu-VirtualBox->/var/log/auth.log
 Sep 22 10:54:28 ubuntu-VirtualBox groupadd[2967]: new group: name=darklord, GID=1001
 Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2
 Sep 22 10:53:57 ubuntu-VirtualBox sshd[2843]: Accepted password for ubuntu from 192.168.56.1 port 58331 ssh2

Level:     3 - Login session opened.                                2020 Sep 22 10:54:11
Rule Id:   5501
Location:  ubuntu-VirtualBox->/var/log/auth.log
 Sep 22 10:54:10 ubuntu-VirtualBox su[2955]: pam_unix(su:session): session opened for user root by ubuntu(uid=0)

Level:     3 - User successfully changed UID to root.               2020 Sep 22 10:54:11
Rule Id:   5303
Location:  ubuntu-VirtualBox->/var/log/auth.log
User:      root
```

2.5. Suspicious port and process launch by "root" user during the incident

```
$ netstat -antp
# Active Internet connections (servers and established)
# Proto Recv-Q Send-Q Local Address Foreign Address State  PID/Program name
# tcp          0      0 0.0.0.0:56565         0.0.0.0:* LISTEN    946/remotesec

$ ps -fp 946
# UID   PID   PPID  C  STIME  TTY  TIME      CMD
# root  946   945   0  06:11  ?    00:00:00  /tmp/remotesec -k -l 56565
```

2.6. Removal of suspicious user and process from the server

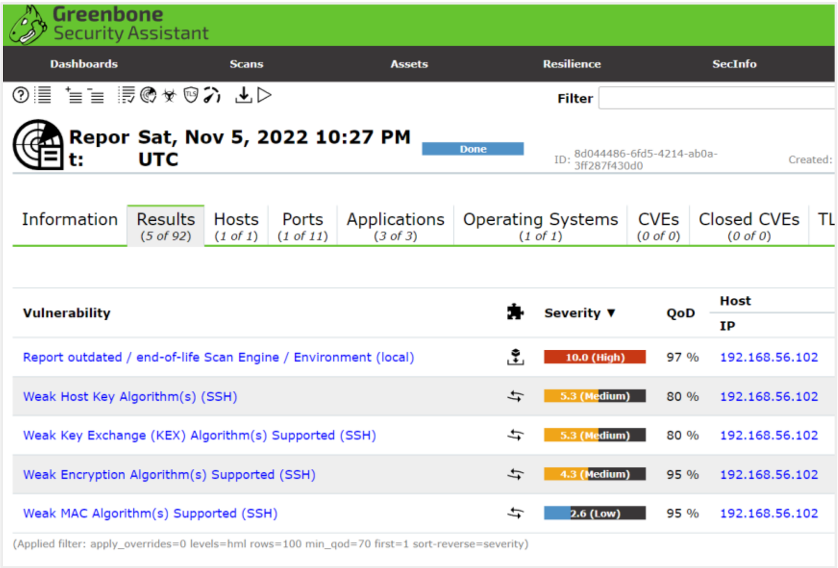
```
$ deluser darklord
$ kill -9 946
```

2.7. SSH configuration for denying access to "root" user through SSH

```
$ vim /etc/ssh/sshd_config
PermitRootLogin no
```

3. SYSTEM HARDENING FOR ENHANCED SECURITY

3.1. OpenVAS Scanning results



Report: Sat, Nov 5, 2022 10:27 PM UTC Done

ID: 8d044486-6fd5-4214-ab0a-3ff287f430d0 Created:

Vulnerability		Severity ▼	QoD	Host IP
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.56.102
Weak Host Key Algorithm(s) (SSH)	⇆	5.3 (Medium)	80 %	192.168.56.102
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	⇆	5.3 (Medium)	80 %	192.168.56.102
Weak Encryption Algorithm(s) Supported (SSH)	⇆	4.3 (Medium)	95 %	192.168.56.102
Weak MAC Algorithm(s) Supported (SSH)	⇆	2.6 (Low)	95 %	192.168.56.102

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

3.2. Hiding Apache Server Metadata

```
$ curl --head localhost
# HTTP/1.1 200 OK
# Date: Sat, 05 Nov 2022 22:57:07 GMT
# Server: Apache/2.4.7 (Ubuntu)

$ vim /etc/apache2/conf-enabled/security.conf
# ServerTokens Minimal
# ServerTokens OS
# ServerTokens Full
ServerTokens Prod
ServerSignature Off
# ServerSignature On

$ sudo service apache2 restart
```

3.3. Creating user for Apache Server

```
$ sudo groupadd apache-group
$ sudo useradd -m apache-user -p [user-password]
$ sudo usermod -aG apache-group apache-user

$ sudo vim /etc/apache2/envvars
export APACHE_RUN_USER=apache-group
export APACHE_RUN_GROUP=apache-user

$ sudo service apache2 restart
```