CYBERSECURITY PROJECT

Presented by Nick Karanja Maina

Introduction

Remote server (209.141.55.128) running Fedora 34

```
C:\Users\hp>nmap -sV 209.141.55.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-04 11:35 E. Africa Standard Time
Nmap scan report for stefan.treylis.org (209.141.55.128)
Host is up (0.060s latency).
Not shown: 992 filtered tcp ports (no-response), 3 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD or KnFTPD
22/tcp  open  ssh         OpenSSH 8.6 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.53 ((Fedora))
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.00 seconds
```

The allocated server was operating in an insecure state without an effective method to ensure total visibility of actions carried out on it.


```
[root@localhost log]# journalctl -r -g "Accepted password for"
Apr 05 09:28:29 localhost.localdomain sshd[144409]: Accepted password for nick from 41.80.10.234 port 4991 ssh2
Apr 05 08:45:59 localhost.localdomain sshd[143121]: Accepted password for nick from 41.80.10.234 port 4747 ssh2
Apr 04 13:58:38 localhost.localdomain sshd[125584]: Accepted password for nick from 197.237.123.154 port 39625 ssh2
Apr 04 13:38:34 localhost.localdomain sshd[125381]: Accepted password for nick from 197.237.123.154 port 39321 ssh2
Apr 04 13:18:44 localhost.localdomain sshd[125137]: Accepted password for nick from 197.237.123.154 port 39033 ssh2
Apr 04 12:54:39 localhost.localdomain sshd[124817]: Accepted password for nick from 197.237.123.154 port 38817 ssh2
Apr 04 12:42:38 localhost.localdomain sshd[124619]: Accepted password for nick from 197.237.123.154 port 38629 ssh2
Apr 04 11:55:12 localhost.localdomain sshd[123960]: Accepted password for nick from 197.237.123.154 port 38038 ssh2
Apr 04 08:06:48 localhost.localdomain sshd[119401]: Accepted password for nick from 105.160.116.10 port 1730 ssh2
Apr 02 10:28:41 localhost.localdomain sshd[95238]: Accepted password for nick from 41.80.13.24 port 1316 ssh2
Apr 01 14:31:13 localhost.localdomain sshd[81140]: Accepted password for nick from 197.237.123.154 port 2640 ssh2
Apr 01 14:04:01 localhost.localdomain sshd[80700]: Accepted password for nick from 197.237.123.154 port 2252 ssh2
Apr 01 13:34:13 localhost.localdomain sshd[79340]: Accepted password for nick from 197.237.123.154 port 1686 ssh2
Apr 01 13:16:18 localhost.localdomain sshd[74903]: Accepted password for nick from 197.237.123.154 port 1387 ssh2
Apr 01 12:22:17 localhost.localdomain sshd[69962]: Accepted password for nick from 197.237.123.154 port 1348 ssh2
Apr 01 11:55:12 localhost.localdomain sshd[69755]: Accepted password for nick from 197.237.123.154 port 2909 ssh2
Apr 01 11:07:06 localhost.localdomain sshd[69358]: Accepted password for nick from 197.237.123.154 port 1042 ssh2
Apr 01 09:27:19 localhost.localdomain sshd[68641]: Accepted password for nick from 41.80.74.2 port 17907 ssh2
Apr 01 08:53:22 localhost.localdomain sshd[67765]: Accepted password for nick from 41.80.74.2 port 17053 ssh2
Apr 01 08:30:25 localhost.localdomain sshd[67491]: Accepted password for nick from 41.80.5.231 port 27246 ssh2
Mar 31 13:23:30 localhost.localdomain sshd[32859]: Accepted password for nick from 41.80.5.231 port 25129 ssh2
Mar 31 11:19:29 localhost.localdomain sshd[27245]: Accepted password for nick from 41.80.5.231 port 42428 ssh2
Mar 31 11:14:01 localhost.localdomain sshd[26954]: Accepted password for nick from 41.80.5.231 port 42016 ssh2
Mar 31 11:01:43 localhost.localdomain sshd[26401]: Accepted password for nick from 41.80.5.231 port 38437 ssh2
Mar 31 09:50:03 localhost.localdomain sshd[18587]: Accepted password for nick from 41.80.5.231 port 31051 ssh2
Mar 31 08:58:33 localhost.localdomain sshd[16221]: Accepted password for nick from 41.80.5.231 port 2581 ssh2
Mar 31 08:46:53 localhost.localdomain sshd[15707]: Accepted password for nick from 41.80.5.231 port 23807 ssh2
Mar 30 12:07:42 localhost.localdomain sshd[9912]: Accepted password for nick from 154.122.9.178 port 9739 ssh2
Mar 30 11:33:47 localhost.localdomain sshd[9830]: Accepted password for nick from 154.122.9.178 port 1615 ssh2
Mar 30 09:45:43 localhost.localdomain sshd[9150]: Accepted password for nick from 41.80.15.93 port 10767 ssh2
Mar 30 09:36:38 localhost.localdomain sshd[8760]: Accepted password for nick from 41.80.15.93 port 21594 ssh2
Mar 30 09:30:05 localhost.localdomain sshd[8392]: Accepted password for root from 197.248.65.18 port 22788 ssh2
```

Unauthorized access via password-based attacks

OSSEC

An open-source HIDS with features such as log-based intrusion detection & file integrity monitoring

Billhacker example:

Minimum level: 2 Category: All categories
Pattern: billhacker Log formats: All log formats
Srcip: User:
Location: Rule id:
Max Alerts: 1000
Search

Results:

Total alerts found: 32

+Severity breakdown
Hiding 19 alert(s) from **level 3** (show)
Hiding 9 alert(s) from **level 10** (show)
Hiding 2 alert(s) from **level 7** (show)
Showing 2 alert(s) from **level 5** (hide) (show only)
Clear level restrictions
+Rules breakdown
+Src IP breakdown

First event at 2022 May 05 10:59:41
Last event at 2022 May 06 08:47:20

Alert list

Level: 5 - **Unauthorized user attempted to use sudo.** 2022 May 06 08:30:45
Rule Id: 5405
Location: localhost->/var/log/secure
May 6 08:30:43 localhost sudo[320315]: billhacker : user NOT in sudoers ; TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash

Level: 5 - **Unauthorized user attempted to use sudo.** 2022 May 06 08:30:27
Rule Id: 5405
Location: localhost->/var/log/secure
May 6 08:30:26 localhost sudo[320306]: billhacker : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/billhacker ; USER=root ; COMMAND=i

OSSEC WebUI
Version 0.8

Main | Search | Integrity checking | Stats | About

April 23rd, 2022 11:14:17 AM

Available agents:

+ossec-server (127.0.0.1)

Latest modified files:

No integrity checking information available.
Nothing reported as changed.

Latest events

Level: 5 - **Web server 400 error code.** 2022 Apr 23 11:10:18
Rule Id: 31101
Location: localhost->/var/log/httpd/access_log
Src IP: 45.155.204.146
45.155.204.146 - - [23/Apr/2022:11:10:17 +0000] "GET /index.php?s=/Index/\\think\\app/invokefunction&function=call_user_func_array&vars[0]=md5&vars[1][]=HelloThinkPHP21 HTTP/1.1" 404 16 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

Level: 5 - **Web server 400 error code.** 2022 Apr 23 10:52:37
Rule Id: 31101
Location: localhost->/var/log/httpd/access_log
Src IP: 41.80.16.116
41.80.16.116 - - [23/Apr/2022:10:52:37 +0000] "GET /HNAP1 HTTP/1.1" 404 196 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

Level: 5 - **Web server 400 error code.** 2022 Apr 23 10:52:37
Rule Id: 31101
Location: localhost->/var/log/httpd/access_log
Src IP: 41.80.16.116
41.80.16.116 - - [23/Apr/2022:10:52:37 +0000] "GET /evox/about HTTP/1.1" 404 196 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

Alert list

Level: 10 - **File added to the system.** 2022 May 06 15:06:06
Rule Id: 554
Location: localhost->syscheck
New file '/home/billhacker/arecord.py.save' added to the file system.
New sha1sum is : 'ee9a1a6b145ed88a8aa0a662c4d8efa5014c90c7'
New md5sum is : '4b1f09efbe953ae88264f2c829e079fd'

May 6 14:48:37 localhost sshd[325857]: Failed password for invalid user mysql from 186.145.109.9 port 34990 ssh2
May 6 14:48:35 localhost sshd[325857]: Invalid user mysql from 186.145.109.9 port 34990
May 6 14:47:40 localhost sshd[325849]: Disconnected from invalid user gustavo 186.145.109.9 port 48986 [preauth]
May 6 14:47:38 localhost sshd[325849]: Failed password for invalid user gustavo from 186.145.109.9 port 48986 ssh2

Level: 10 - **File added to the system.** 2022 May 06 12:54:13
Rule Id: 554
Location: localhost->syscheck
New file '/home/billhacker/arecord.py' added to the file system.
New sha1sum is : 'da39a3ee5e6b4b0d3255bfef95601890afd80709'
New md5sum is : 'd41d8cd98f00b204e9800998ecf8427e'

Level: 10 - **File added to the system.** 2022 May 06 12:37:43
Rule Id: 554
Location: localhost->syscheck
New file '/home/billhacker/pkexec' added to the file system.
New sha1sum is : '30b8580a9b170c30556b895d4a8a86a2c2cd15d0'
New md5sum is : '5a37e75390a98d5fe2395f553feb921d'

Old sha1sum was: '7c2d5dc6bc39084d856760fc8c315420bca60317'
New sha1sum is : '3e300c3741d90a8c16e916dbee483afe4acbb608'

May 6 12:16:50 localhost sshd[324199]: Failed password for root from 41.242.112.44 port 58280 ssh2

Level: 4 - First time user logged in.
Rule Id: 10100
Location: localhost->/var/log/secure
Src IP: 43.154.39.203
User: hacker

2022 May 10 04:23:05

May 10 04:23:04 localhost sshd[391500]: Accepted password for hacker from 43.154.39.203 port 38860 ssh2

Further Indicators vs Response

Files added

Level: 10 - File added to the system.
Rule Id: 554
Location: localhost->syscheck

New file '/home/hacker/.configrc/a/kswapd0' added to the file system.
New sha1sum is : '7f751ed078b431cb82a71584a48e7ef065264e81'
New md5sum is : '2f7f5fb5de175e770d7eae87666f9831'

Resources in use

```
top - 09:06:11 up 37 days, 23:02,  2 users,  load average: 8.96, 18.20, 24.38
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
%Cpu(s): 97.3 us,  1.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  1.0 hi,  0.7 si,  0.0 st
MiB Mem :    959.3 total,     74.4 free,    518.6 used,    366.4 buff/cache
MiB Swap:    959.0 total,    810.8 free,    148.1 used.    294.9 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 968095 hacker    20   0  714132 263884      0 S  92.4  26.9   1121:27 kswapd0
 988313 hacker    20   0 4783332  10948   1104 S   5.6   1.1   5:51.58 tsm
```

Random connections opened

```
tcp    SYN-SENT   0      1                                  209.141.55.128:47290          139.210.243.102:ssh
tcp    SYN-SENT   0      1                                  209.141.55.128:42080           18.179.23.66:ssh
tcp    ESTAB      0      84                                 209.141.55.128:40482          81.169.224.227:ssh
```

Changed account password

```
Changing password for user hacker.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Killed processes

```
[root@localhost rules]# pkill -9 -u hacker
```

Deleted files

```
[root@localhost .ssh]# nano authorized_keys
[root@localhost .ssh]# less authorized_keys
[root@localhost .ssh]# rm authorized_keys
rm: remove regular empty file 'authorized_keys'? y
```

Resources no longer tied

```
    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
1051811 root      20   0   20148   4256   3624 R   0.3   0.4   0:00.05 top
      1 root      20   0  184576   7992   5012 S   0.0   0.8   3:47.19 systemd
```

Level: 5 - SSHD authentication failed.
Rule Id: 5716
Location: localhost->/var/log/secure
Src IP: 37.116.206.113
User: root
Aug 11 15:12:49 localhost sshd[519633]: Failed password for root from 37.116.206.113 port 42184 ssh2

Level: 5 - SSHD authentication failed.
Rule Id: 5716
Location: localhost->/var/log/secure
Src IP: 37.116.206.113
User: root
Aug 11 15:12:46 localhost sshd[519633]: Failed password for root from 37.116.206.113 port 42184 ssh2

Level: 5 - SSHD authentication failed.
Rule Id: 5716
Location: localhost->/var/log/secure
Src IP: 37.116.206.113
User: root
Aug 11 15:12:39 localhost sshd[519633]: Failed password for root from 37.116.206.113 port 42184 ssh2

SSH configuration and username change

Level: 3 - SSHD authentication success.
Rule Id: 5715
Location: localhost->/var/log/secure
Src IP: 41.80.2.1
User: nickphaita
Jul 2 07:54:50 localhost sshd[210061]: Accepted password for nickphaita from 41.80.2.1 port 44414 ssh2

Level: 3 - Login session opened.
Rule Id: 5501
Location: localhost->/var/log/secure
Jul 2 07:54:50 localhost sshd[210061]: pam_unix(sshd:session): session opened for user nickphaita(uid=1000) by (uid=0)

CIS Center for Internet Security®

Uninstall services and close ports that aren't in use

```
80/tcp   open   http        Apache httpd 2.4.53 ((Fedora))
```

```
ServerTokens Prod
ServerSignature Off
```

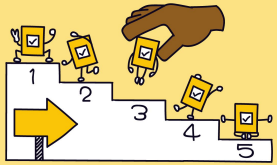
```
80/tcp open  http    Apache httpd
```

Apache configuration

```
C:\Users\hp>nmap -sV 209.141.55.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 13:13 E. Africa Standard Time
Nmap scan report for stefan.treylis.org (209.141.55.128)
Host is up (0.13s latency).
Not shown: 986 filtered tcp ports (no-response), 11 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.6 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.53 ((Fedora))
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.82 seconds
```

Key takeaways:



Categorize assets and threats in order of priority

Have complete visibility of your environment

Maintain an appropriate security policy

Establish a suitable incident response plan