Hammered Lab (Cyber Defenders) - Walkthrough

Thursday, September 19, 2024 12:20 PM

Story:
This challenge takes you into the world of virtual systems and confusing log data. In this challenge, as a soc analyst figure out what happened to this webserver honeypot using the logs from a possibly compromised server.

Q1: Which service did the attackers use to gain access to the system?

- To address this question, I accessed to 'auth.log' and searched 'failure' as a keyword.
  I identified BT activity on the **SSH service.**

Q2: What is the operating system version of the targeted system? (one word)

- To address this question, I accessed to 'dmesg' log which contains messages from the kernel ring buffer, primarily related to system boot and hardware events.
  And found the version is '4.2.4-1ubuntu3'

```
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Linux version 2.6.24-26-server (buildd@crested) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu3)) #1 SMP Tue Dec 1 18:26:43 UTC 2009 (Ubuntu 2.6.24-26.64-server)
[    0.000000] Command line: root=UUID=a691743a-a4b7-482d-95ff-406e5acd83a3 ro quiet splash
[    0.000000] BIOS-provided physical RAM map:
[    0.000000]  BIOS-e820: 0000000000000000 - 000000000009f800 (usable)
[    0.000000]  BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)
```

Q3: What is the name of the compromised account?

- All the BT attempts performed on 'Root' user.

Q4: Consider that each unique IP represents a different attacker. How many attackers were able to get access to the system?

- First of all the filtered all the IPs that logged in to root user via the command:
  cat auth.log | grep Accept | grep 'root' | cut -d ' ' -f 11 | sort -u

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat auth.log | grep Accept | grep 'root' | cut -d ' ' -f 11 | sort -u
10.0.1.2
121.11.66.70
122.226.202.12
151.81.204.141
151.81.205.100
151.82.3.201
188.131.22.69
188.131.23.37
190.166.87.164
190.167.70.87
190.167.74.184
193.1.186.197
201.229.176.217
219.150.161.20
222.169.224.197
222.66.204.246
61.168.227.12
94.52.185.9
```

After I filtered all the failure attempts to identified which of the addresses related to BT:
cat auth.log | grep failure | grep 'root' | cut -d ' ' -f 14 | sed 's/rhost=//' | sort | uniq -c | sort -nr

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat auth.log | grep failure | grep 'root' | cut -d ' ' -f 14 | sed 's/rhost=//' | sort | uniq -c | sort -nr
   1560 219.150.161.20
   1429 121.11.66.70
    508 222.66.204.246
    313 122.226.202.12
    246 58.17.30.49
    193 61.168.227.12
    179 222.169.224.197
    122 124.207.117.9
    121 209.59.222.166
    113 116.6.19.70
     97 8.12.45.242
     78 mail.mediamonitors.com.pk
     73 114.80.166.219
     71 211.154.254.248
     48 jp.user2pastoreinc.com
     48 201.64.234.2
     44 217.15.55.133
     42 59.46.39.148
     34 122.102.64.54
     28 219.139.243.236
     26 200.72.254.54
     24 125.235.4.130
     15 d192-24-91-113.try.wideopenwest.com
     13 61.151.246.140
     13 220.170.79.247
     10 190.4.21.190
```

Now, we have 2 lists, I sent it to ChatGPT to compare between them and we received:

121.11.66.70 (1429 attempts)
122.226.202.12 (313 attempts)
219.150.161.20 (1560 attempts)
222.66.204.246 (508 attempts)
61.168.227.12 (193 attempts)

222.169.224.197 (179 attempts)

All these addresses related to BT and logged in successfully.

Q5:Which attacker's IP address successfully logged into the system the most number of times?

- I used the same method as above and found the address '**219.150.161.20**', which is related to the attacker logging in to the root user four times.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat auth.log| grep -i accept | grep root | cut -d ' ' -f 11 | sort | uniq -c | sort -nr
      6 :
      4 219.150.161.20
      4 188.131.23.37
      3 190.166.87.164
      2 122.226.202.12
      2 121.11.66.70
      1 94.52.185.9
      1 61.168.227.12
      1 222.66.204.246
      1 222.169.224.197
      1 201.229.176.217
      1 193.1.186.197
      1 190.167.74.184
      1 190.167.70.87
      1 188.131.22.69
      1 151.82.3.201
      1 151.81.205.100
      1 151.81.204.141
      1 10.0.1.2
```

Q6: How many requests were sent to the Apache Server?

- I count the access log via 'wc -l'

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat www-access.log | wc -l
365
```

Q7: How many rules have been added to the firewall?

- **In the 'Auth.log' file we are able to see the attacker commands, I identified the threat-actor added '6' rules to the FW**

```
Line  94954: Apr 24 20:03:06 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p ssh -dport 2424 -j ACCEPT
Line  94957: Apr 24 20:03:44 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p tcp -dport 53 -j ACCEPT
Line  94960: Apr 24 20:04:13 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p udp -dport 53 -j ACCEPT
Line  94967: Apr 24 20:06:22 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p tcp --dport ssh -j ACCEPT
Line  94972: Apr 24 20:11:00 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p tcp --dport 53 -j ACCEPT
Line  94979: Apr 24 20:11:08 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p tcp --dport 113 -j ACCEPT
```

Q8: One of the downloaded files to the target system is a scanning tool. Provide the tool name.

- I assumed the answer was 'Nmap,' but I used the 'Term.log' file, which tracks installed packages. I found that 'Nmap' was unpacked.

```
Line 371: Unpacking libgnomecanvas2-0 (from .../libgnomecanvas2-0_2.20.1.1-1_amd64.deb) ...
Line 373: Unpacking libbonoboui2-0 (from .../libbonoboui2-0_2.21.90-1_amd64.deb) ...
Line 375: Unpacking libgnomeui-common (from .../libgnomeui-common_2.22.1.0-0ubuntu2_all.deb) ...
Line 377: Unpacking libgnomeui-0 (from .../libgnomeui-0_2.22.1.0-0ubuntu2_amd64.deb) ...
Line 379: Unpacking firestarter (from .../firestarter_1.0.3-6ubuntu3_amd64.deb) ...
Line 592: Unpacking nmap (from .../archives/nmap_4.53-3_amd64.deb) ...
Line 600: Unpacking replacement dpkg ...
Line 605: Unpacking replacement tzdata ...
Line 616: Unpacking replacement libkrb53 ...
Line 618: Unpacking replacement exim4-config ...
Line 620: Unpacking replacement exim4-base ...
Line 624: Unpacking replacement exim4-daemon-light ...
```

Q9: When was the last login from the attacker with IP 219.150.161.20? Format: MM/DD/YYYY HH:MM:SS AM

- To address this question, I filtered the auth.log by the attacker's IP and searched for the last login. I found that the last login from this IP was at 'Apr 19 05:56:05', but we don't know the year. I accessed dpkg.log, which gave me an indication of the year (2010).

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat auth.log | grep '219.150.161.20' | grep 'Accept'
Apr 19 05:41:44 app-1 sshd[8810]: Accepted password for root from 219.150.161.20 port 51249 ssh2
Apr 19 05:42:27 app-1 sshd[9031]: Accepted password for root from 219.150.161.20 port 40877 ssh2
Apr 19 05:55:20 app-1 sshd[12996]: Accepted password for root from 219.150.161.20 port 55545 ssh2
Apr 19 05:56:05 app-1 sshd[13218]: Accepted password for root from 219.150.161.20 port 36585 ssh2
```

Q10: The database displayed two warning messages, provide the most important and dangerous one.

- The **daemon.log** file is a log file used in Linux systems to capture messages from various system daemons.
  These daemons are background processes that handle tasks and services, such as system management, scheduling, and networking.

  I navigated through the log file and noticed MySQL logs.
  After several minutes, I found the answer:

```
Apr 14 14:44:34 app-1 /etc/mysql/debian-start[5364]: Checking for insecure root accounts.
Apr 14 14:44:34 app-1 /etc/mysql/debian-start[5369]: WARNING: mysql.user contains 2 root accounts without password!
Apr 14 14:44:34 app-1 /etc/mysql/debian-start[5370]: Checking for crashed MySQL tables.
```

Q11: Multiple accounts were created on the target system. Which one was created on Apr 26 04:43:15?

- I filtered the access.log by the mentioned date.

```
Search "Apr 26 04:43:15" (2 hits in 1 file of 1 searched) [Normal]
  C:\Users\FlareVM\Desktop\Hammered\auth.log (2 hits)
    Line  99679: Apr 26 04:43:15 app-1 groupadd[20114]: new group: name=wind3str0y, GID=1005
    Line  99680: Apr 26 04:43:15 app-1 useradd[20115]: new user: name=wind3str0y, UID=1004, GID=1005, home=/home/wind3str0y, shell=/bin/bash
Search "warning" (25 hits in 2 files of 18 searched) [Normal]
```

Q12: Few attackers were using a proxy to run their scans.
What is the corresponding user-agent used by this proxy?

- I used the grep utility to filter only the start of the user agent (like the answer format) and found the suspicious user agent 'pxyscand/2.1'.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat www-access.log| cut -d ' ' -f 12 | sort | uniq
"-"
"Apple-PubSub/65.12.1"
"Mozilla/4.0
"Mozilla/5.0
"pxyscand/2.1"
"WordPress/2.9.2;
```