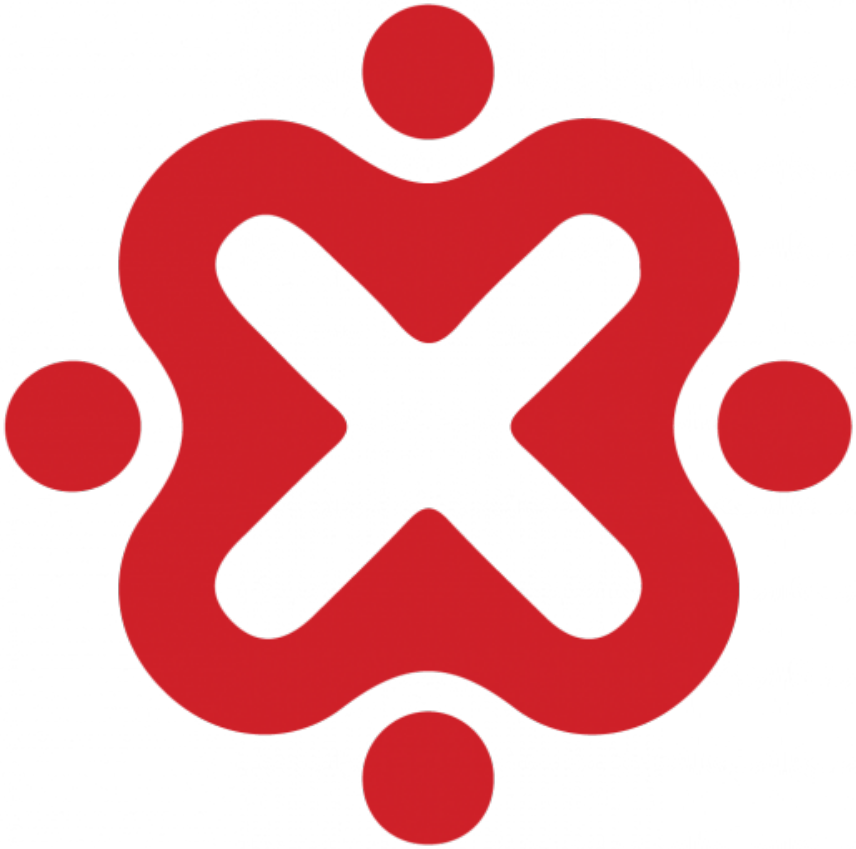
Praktikum

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.

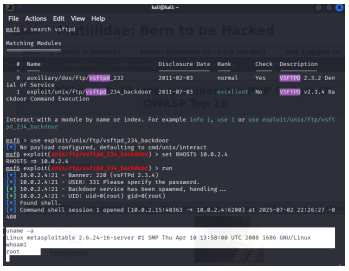
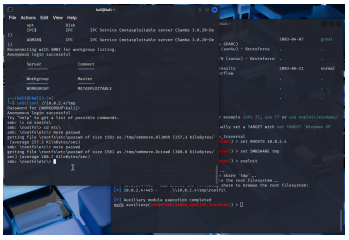
d. Pelaporan (*Reporting*): Menyusun laporan hasil pengujian dan memberikan rekomendasi mitigasi.

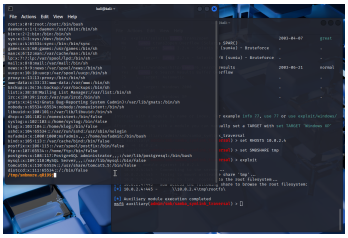
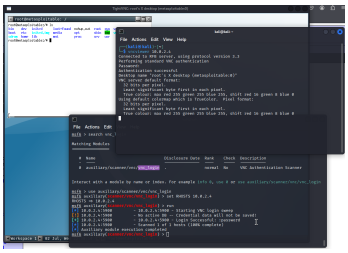
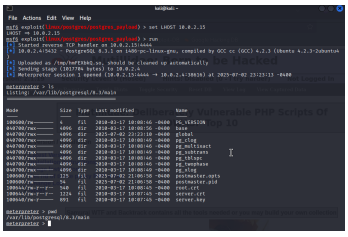
5. Langkah-Langkah Praktikum

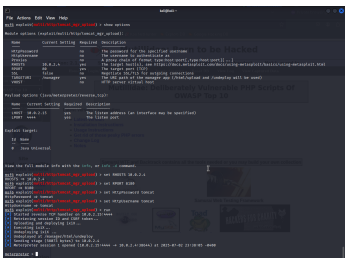
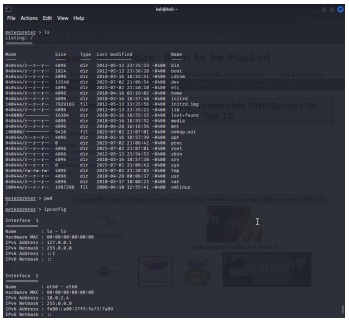
Langkah-langkah yang dilakukan dalam pengujian berdasarkan metodologi yang digunakan:

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 eksploitasi 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	*FTP Exploitation* (Port 21) [CVE-2011-2523 – *Backdoor (malicious code injection)*, CWE-912 – *Hidden Functionality* (*Backdoor*), CWE-77 – *Command Injection*]	Terdapat *backdoor* pada layanan vsftpd versi 2.3.4 yang berasal dari kode sumber resmi. *Backdoor* disisipkan oleh pihak ketiga yang tidak sah ke dalam kode sumber resmi. *Backdoor* tersebut memicu *shell bind* pada port TCP tertentu (biasanya 6200) yang bisa digunakan untuk mendapatkan akses *remote shell* sebagai *root.*	Dampak yang ditimbulkan oleh kerentanan ini adalah *Remote Code Execution (RCE), Privilege Escalation,* dan *Backdoor Access.*	
2	*Samba Exploitation* (Port 23) [CWE-22 – *Path Traversal*, CWE-59 – *Link Following*]	Kerentanan pada konfigurasi Samba yang tidak memeriksa dengan benar penggunaan *symbolic link* (*symlink*) di dalam direktori yang dibagikan (*share*). Aktif secara *default* Samba	Dampak yang ditimbulkan oleh kerentanan ini adalah *Unauthorized File Access, Information Disclosure, Post-exploitation Support,*	

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

5	*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*]	Layanan Apache Tomcat menggunakan konfigurasi *Tomcat Manager Application* yang rentan dengan kredensial *default* dan mengizinkan pengunggahan *file web shell (WAR file)* ke *server*. Hal tersebut memungkinkan untuk serangan *Remote Code Execution (RCE)*. Kerentanan layanan ini dapat dieksploitasi dengan modul metasploit-framework *tomcat_mgr_upload.*	Dampak yang dapat ditimbulkan oleh kerentanan ini adalah *Remote Code Execution (RCE), Reverse Shell Access* (mendapatkan *shell* interaktif), *System Enumeration* (seperti melihat, mencuri atau mengeksekusi file), *Persistence (backdoor)*, dan *Privilege Escalation*.	 

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 – U*se 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 – U*nrestricted 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.

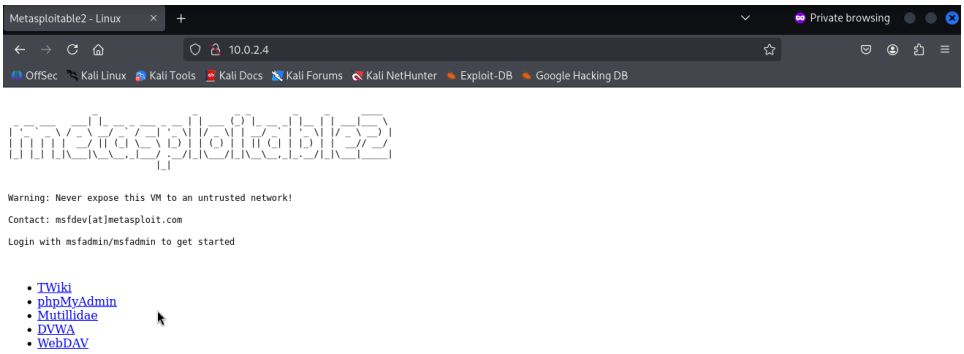
- Apakah ada tools/metode yang tidak berjalan sesuai ekspektasi?

  Tidak ada, semua berjalan dengan semestinya dan sesuai harapan.

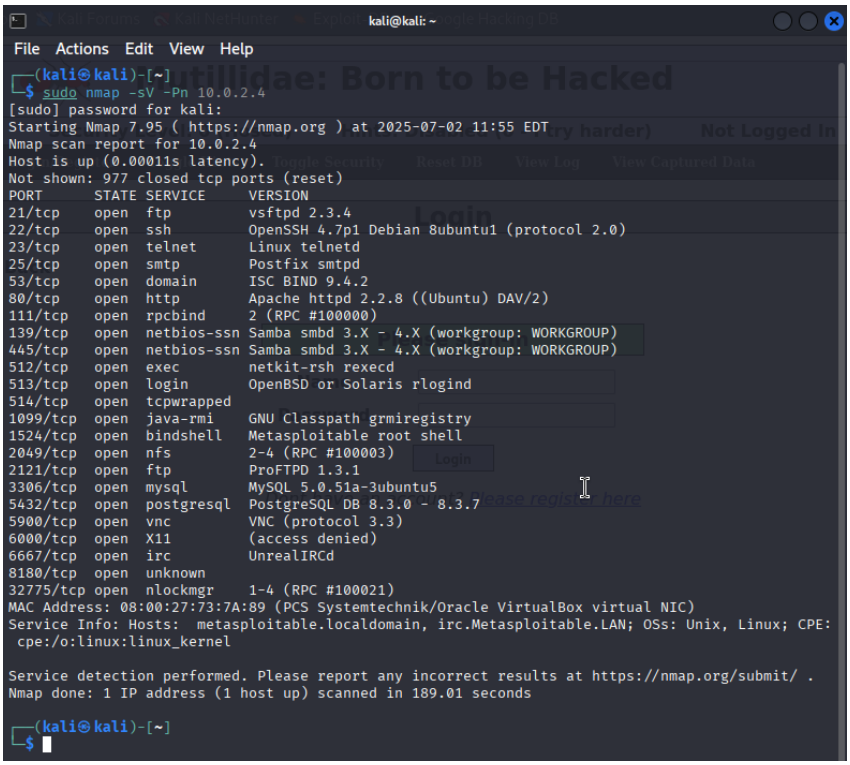
- Apa pelajaran paling penting yang dipelajari dari praktikum ini?

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

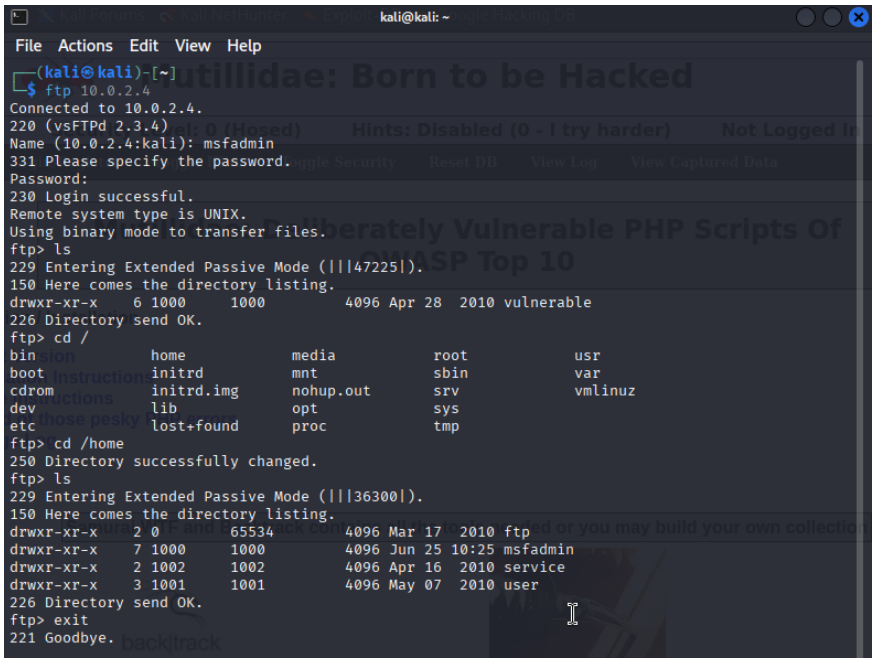
9. Lampiran



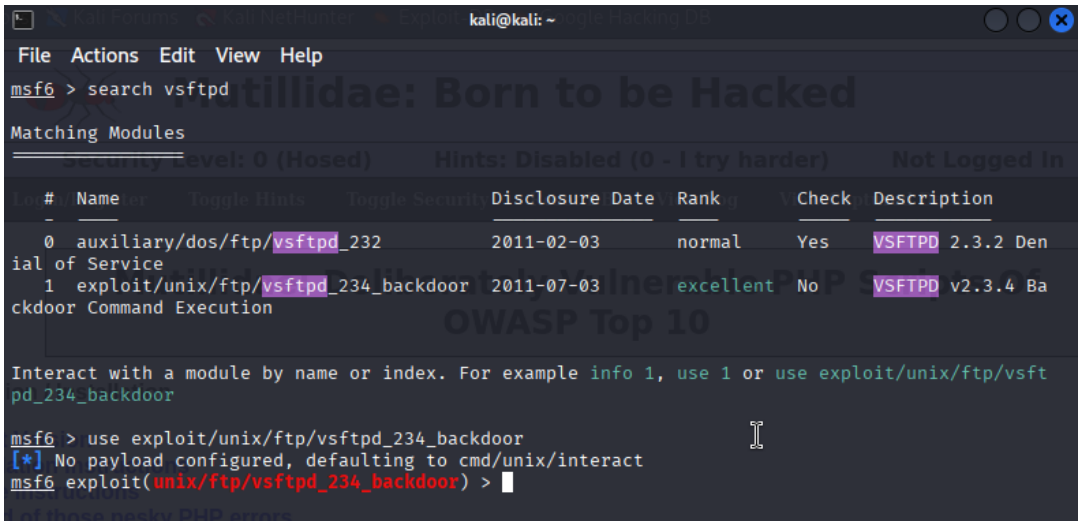
Gambar 1: Halaman Utama Metasploitable 2 diakses dari Peramban Web



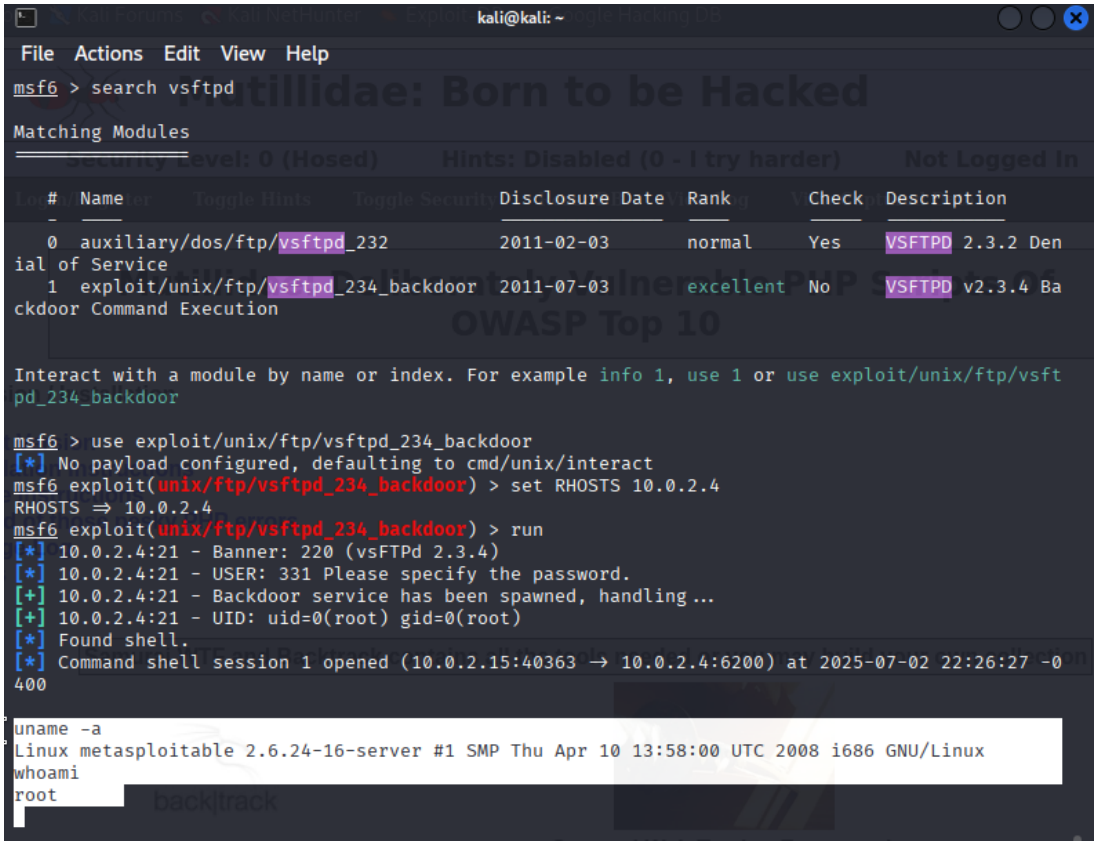
Gambar 2: Pemindaian Layanan yang Tersedia di *Server* Metasploitable 2 dengan nmap



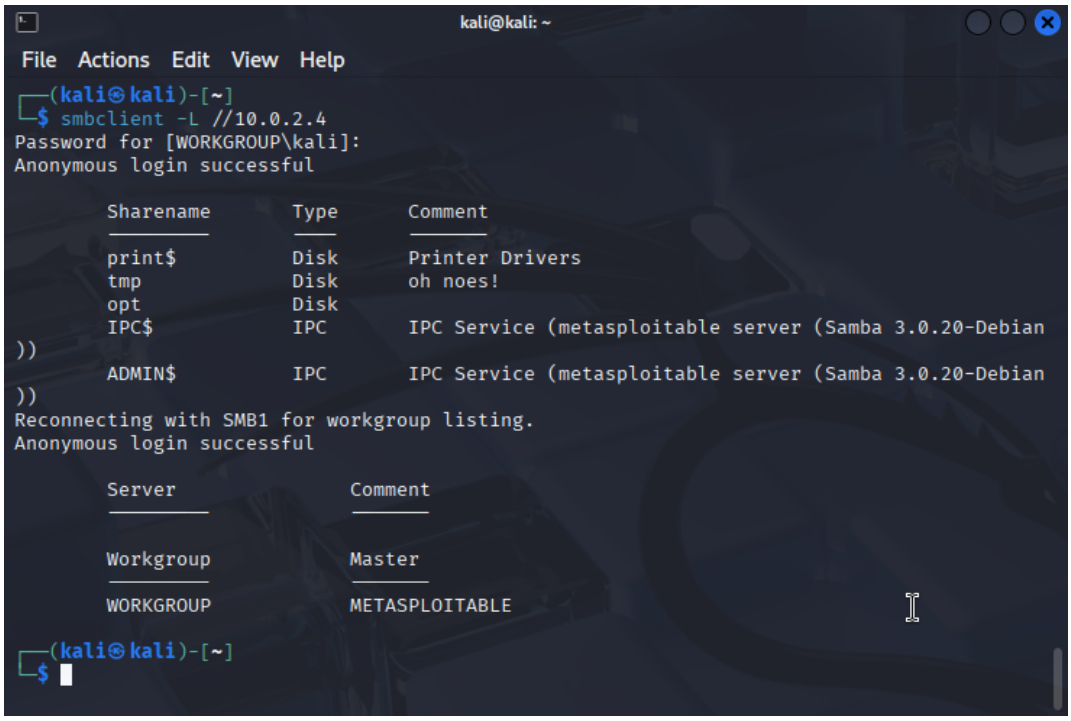
Gambar 3: Uji Coba Akses Layanan FTP Metasploitable 2



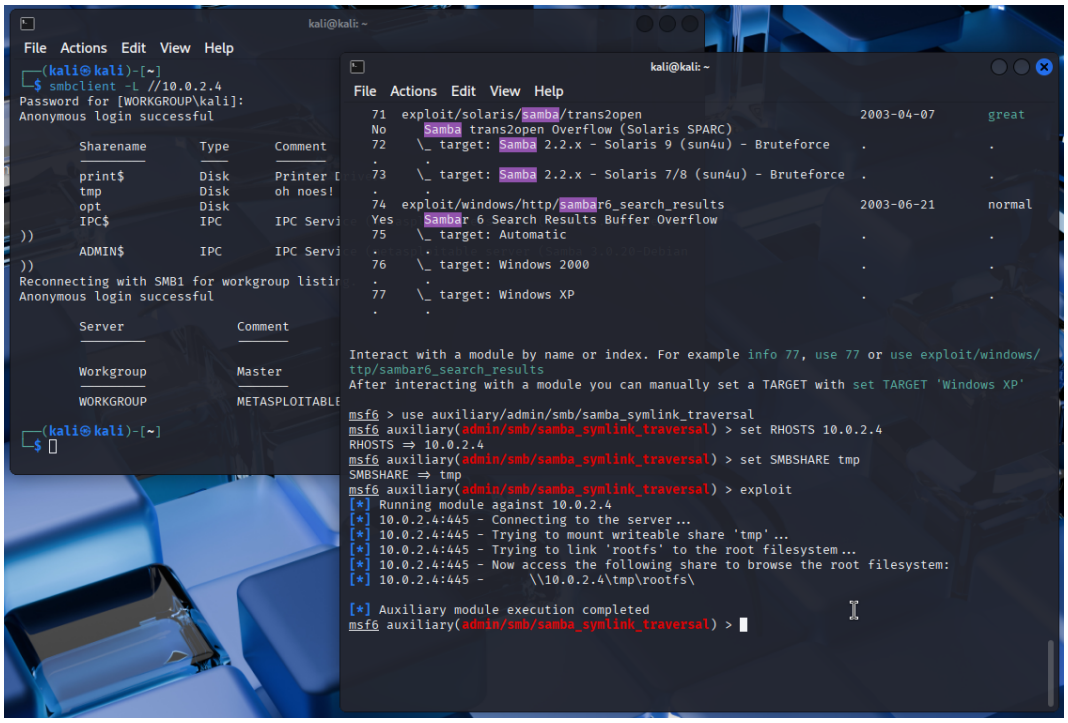
Gambar 4: *FTP Exploitation* - Mencari dan Menggunakan Modul Eksploitasi untuk Layanan FTP pada *metasploit-framework*



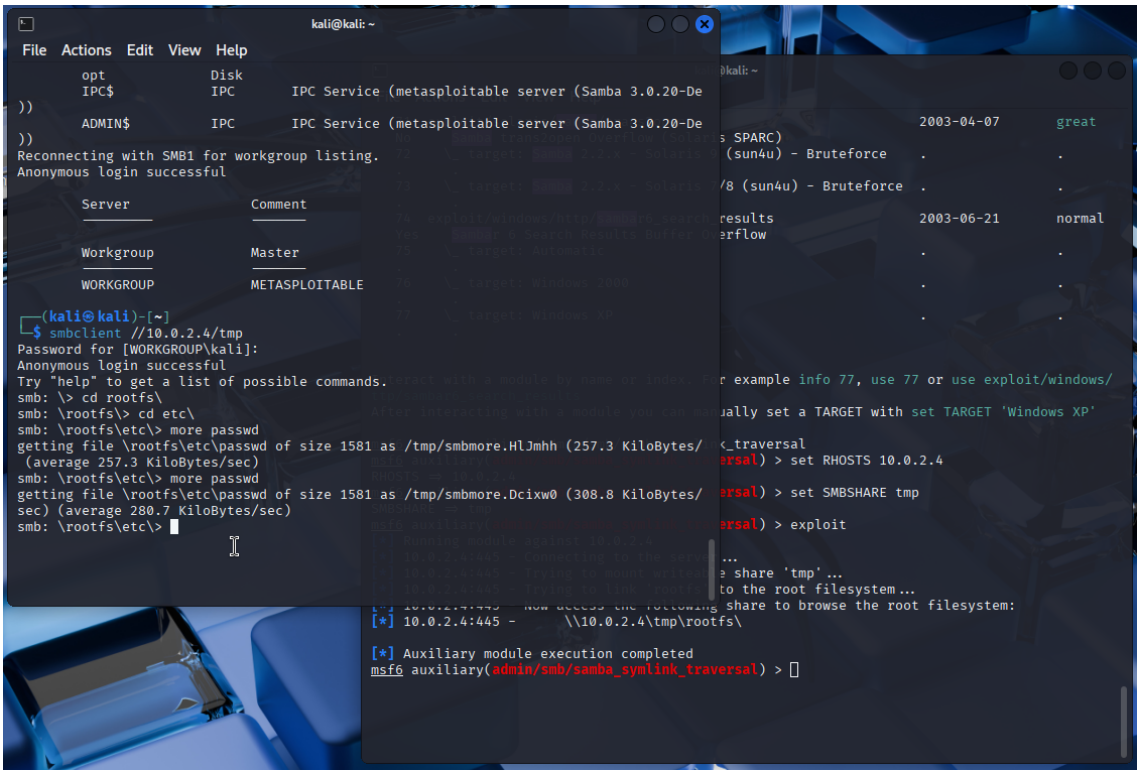
Gambar 5: *FTP Exploitation* - Eksploitasi Kerentanan FTP dengan Modul dari *metasploit-framework*



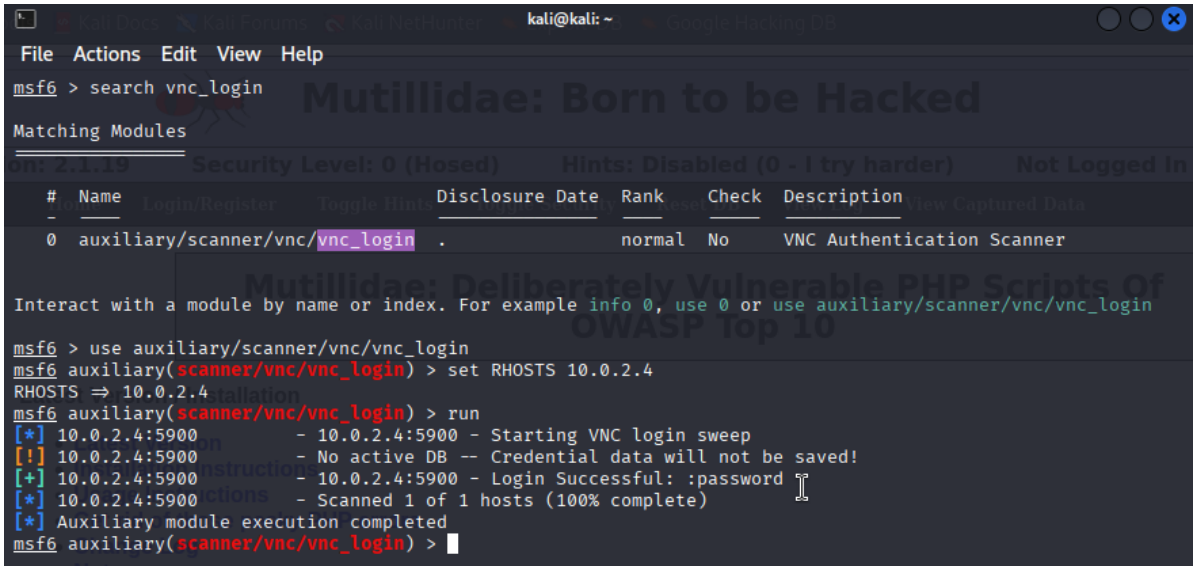
Gambar 6: *Samba Exploitation* - Memeriksa *sharename* yang Tersedia



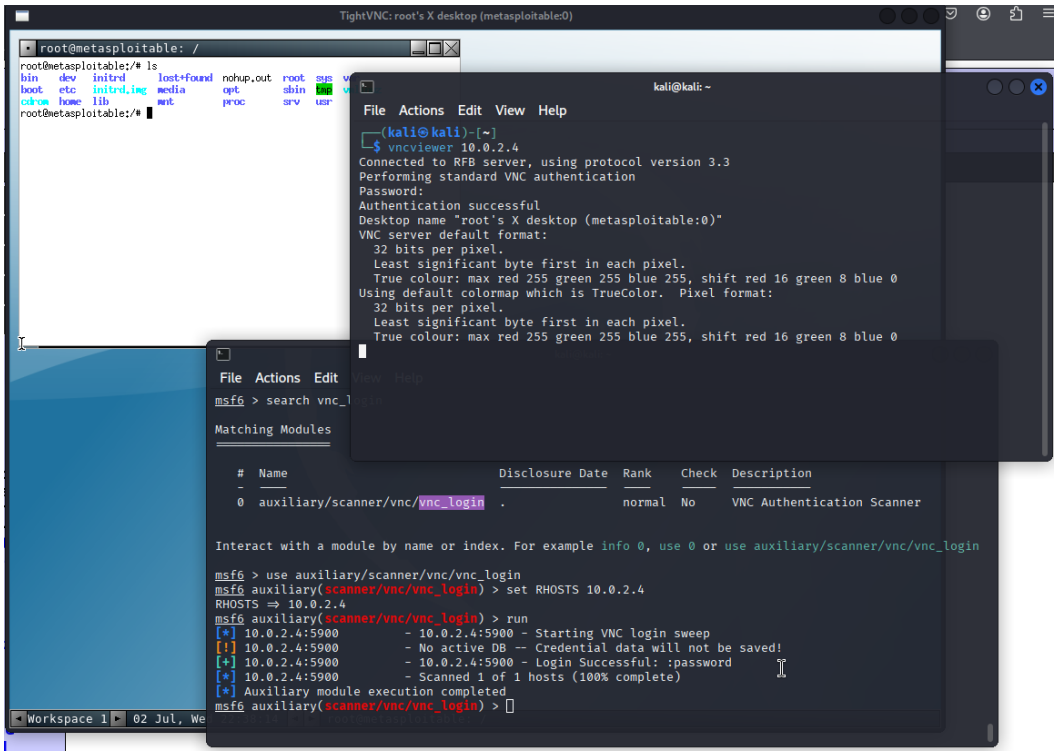
Gambar 7: *Samba Exploitation* - Mencari Modul Eksploitasi pada *metasploit-framework* dan Menggunakannya



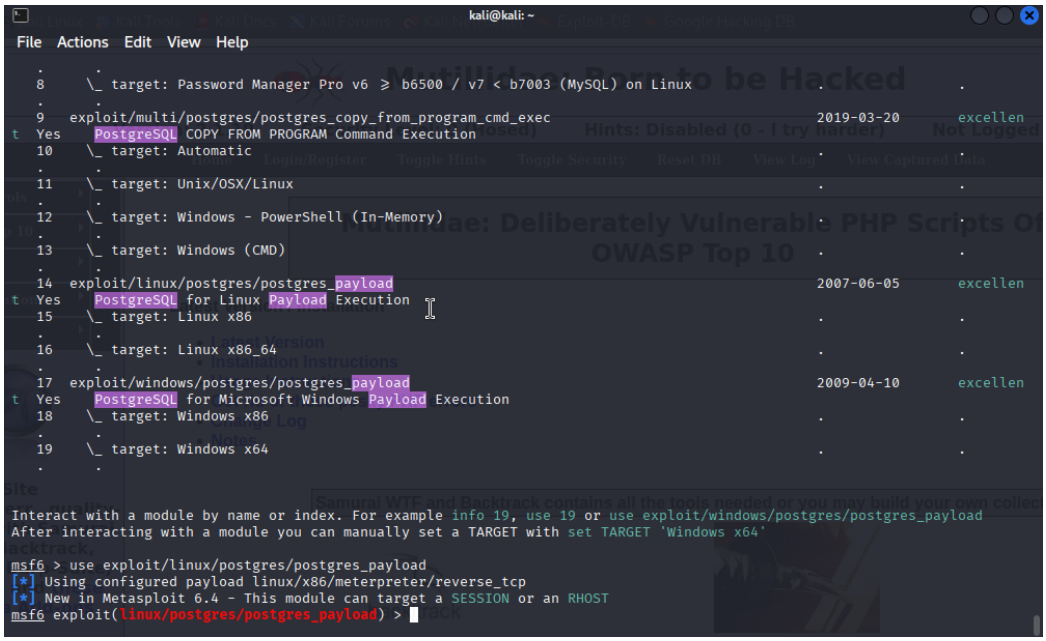
Gambar 8: *Samba Exploitation* - Menguji Hasil Eksploitasi dari Modul *metasploit-framework*



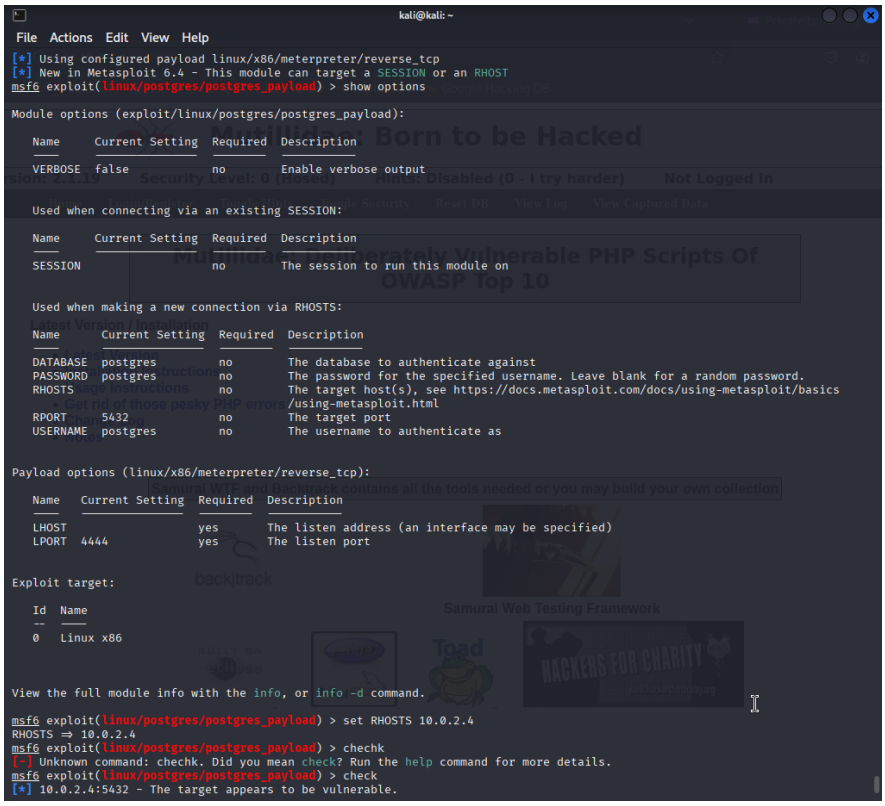
Gambar 9: *VNC Exploitation* - Mencari Modul Eksploitasi pada *metasploit-framework* dan Menggunakannya



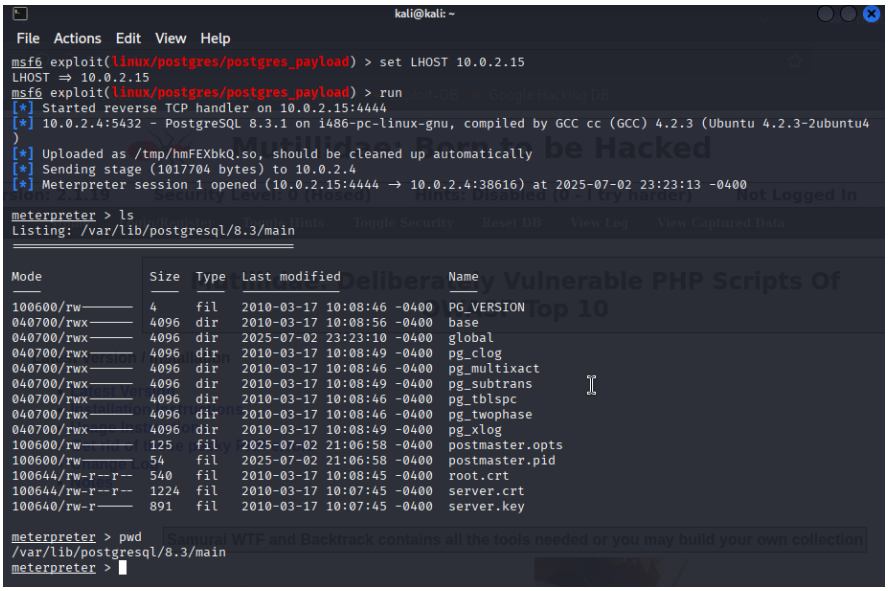
Gambar 10: ***VNC Exploitation*** **- Menguji Hasil Eksploitasi dari Modul** ***metasploit-framework***



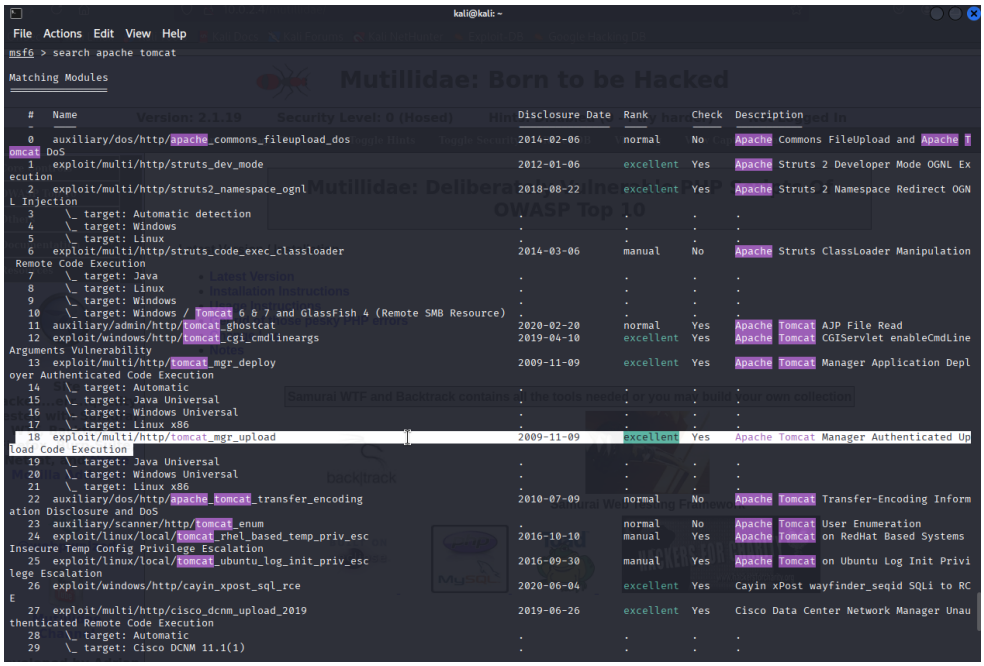
Gambar 11: ***PostgreSQL Exploitation*** **- Mencari Modul Eksploitasi pada** ***metasploit-framework*** **dan Menggunakannya**



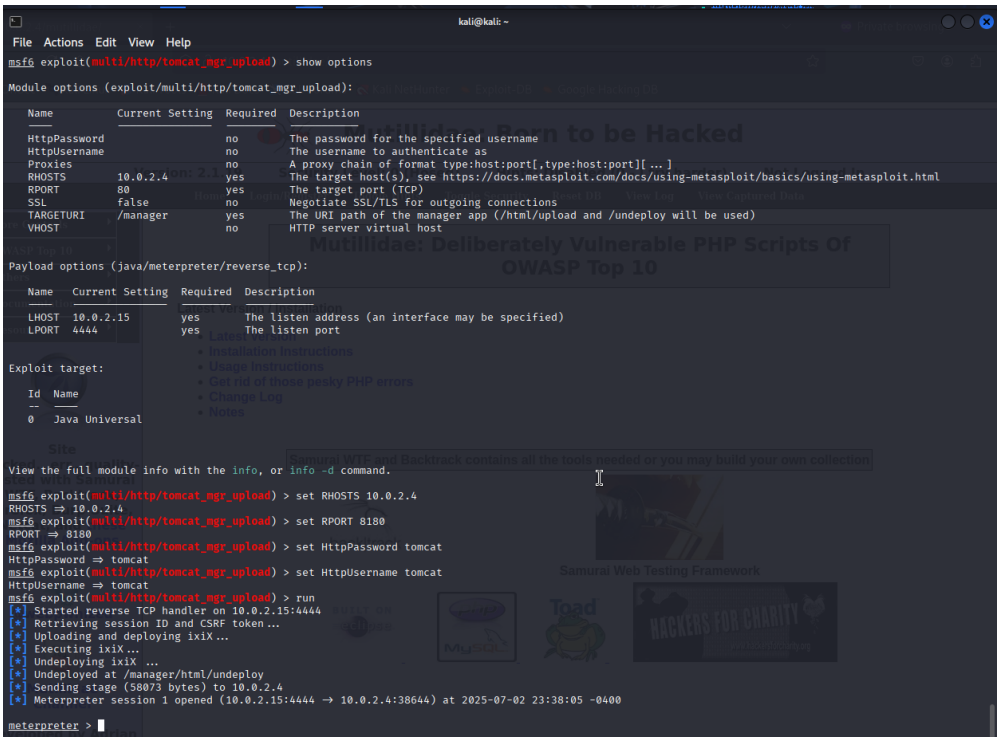
Gambar 12: *PostgreSQL Exploitation* - Melihat Pilihan pada Modul Eksploitasi dan Menentukan *Host* Target



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



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



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

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