LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Pertemuan 8

Footprinting & Reconnaissance

DISUSUN OLEH

Nama	: Sofiyanatul Munawaroh
NIM	: 21/474781/SV/19035
Hari, Tanggal	: Selasa, 2 Mei 2023
Kelas	: RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK

PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI

REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Praktikum Keamanan Informasi 1

Pertemuan 8 – *Footprinting & Reconnaissance*

I. Tujuan

- Dapat memindai jaringan target untuk menentukan semua kemungkinan *port* terbuka, *host* langsung, dan layanan yang berjalan.
- Mengetahui tentang teknik pembuatan paket yang membantu untuk memindai jaringan di luar *firewall* atau IDS.
- Mengumpulkan informasi tentang target atau sistem yang akan diserang.

II. Latar Belakang

Footprinting adalah proses pengumpulan informasi tentang suatu target dengan tujuan untuk memahami infrastruktur jaringan, sistem, dan sasaran yang akan diserang. Salah satu teknik yang dapat digunakan dalam *footprinting* adalah teknik *crafting* UDP dan TCP *packet* menggunakan alat seperti hping3.

Hping3 adalah alat yang serbaguna untuk pengujian dan pengeksploitasi jaringan. Dengan hping3, kita dapat membuat, mengirim, dan menganalisis paket jaringan, termasuk paket UDP dan TCP, dengan kontrol yang lebih tinggi dibandingkan dengan alat-alat lainnya. Dengan menggunakan hping3, peneliti keamanan dapat melakukan *footprinting* melalui teknik *crafting* paket yang disesuaikan dengan tujuan mengumpulkan informasi tentang target.

Teknik *crafting* UDP dan TCP *packet* menggunakan hping3 dapat digunakan untuk mengirim paket dengan opsi-opsi yang dikustomisasi untuk menguji kerentanan dan perilaku sistem target, memeriksa apakah *port-port* tertentu pada target terbuka atau tertutup, serta menganalisis respons dari target untuk mengidentifikasi kelemahan atau celah keamanan.

Reconnaissance adalah proses pengumpulan informasi tentang target atau sistem yang bertujuan untuk memperoleh pemahaman yang lebih baik tentang infrastruktur jaringan, sistem, layanan yang berjalan, kerentanan yang mungkin ada, dan informasi lainnya yang dapat digunakan untuk merencanakan serangan yang efektif atau pengujian keamanan.

Reconnaissance dapat dilakukan oleh penyerang yang memiliki niat jahat atau oleh peneliti keamanan yang bertujuan untuk mengidentifikasi dan mengatasi kerentanan dalam sistem. Tujuan utama *reconnaissance* adalah memperoleh informasi yang cukup untuk merencanakan langkah-langkah selanjutnya dalam serangan atau pengujian keamanan.

Proses *reconnaissance* dapat mencakup langkah-langkah seperti pencarian informasi public, *scanning*, *footprinting*, dan analisis trafik jaringan.

III. Alat dan Bahan

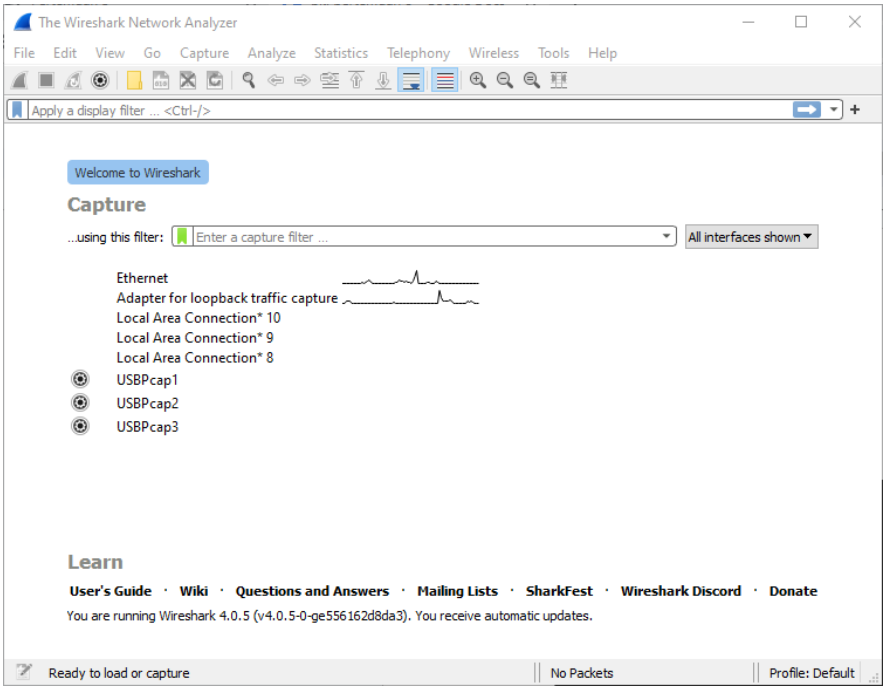
- *Software Remote Desktop Connection*
- *Wireshark*
- Kali Linux
- Laptop/PC

- Koneksi Internet

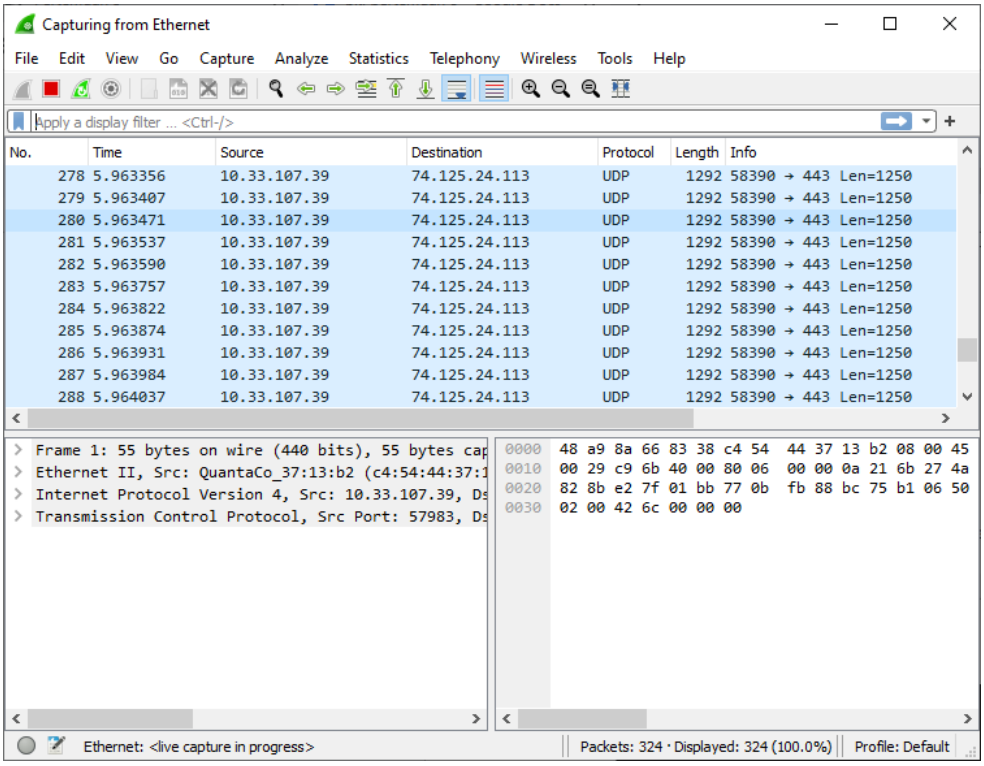
IV. Instruksi Kerja

A. Teknik *Crafting* UDP dan TCP *Packets* menggunakan Hping3

1. Buka *server* windows *Start* → *All Apps* dan klik *Wireshark* untuk memulai aplikasi.



2. Jendela utama *Wireshark* muncul. Klik dua kali pada *Ethernet* untuk mulai menangkap paket.



3. *Wireshark* mulai menangkap lalu lintas pada antarmuka *Ethernet.*
4. Masuk ke VM kalilinux.

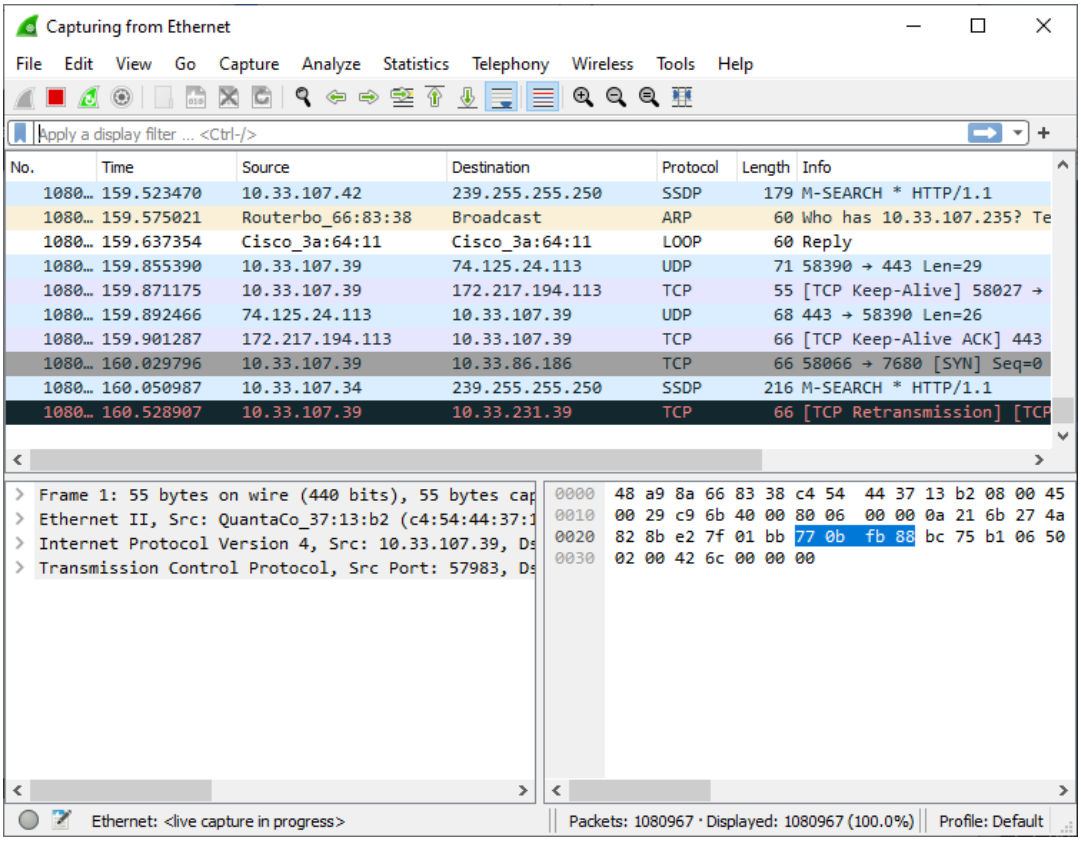
5. Cek IP PC pada *Command Prompt*.

```
C:\Users\TAJ>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6201:a8e4:4141:6bc5%6
   IPv4 Address. . . . . . . . . . . : 10.33.107.39
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.33.107.254

C:\Users\TAJ>
```

6. Buka terminal, masuk ke direktori *root*, dan ketik **hping3 -c 3 10.33.107.39** dan tekan *Enter*. (IP merupakan IP PC Windows).

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -c 3 10.33.107.39
HPING 10.33.107.39 (eth0 10.33.107.39): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.33.107.39 ttl=127 DF id=51178 sport=0 flags=RA seq=0 win=0 rtt=13.1 ms
len=46 ip=10.33.107.39 ttl=127 DF id=51410 sport=0 flags=RA seq=1 win=0 rtt=12.8 ms
len=46 ip=10.33.107.39 ttl=127 DF id=51501 sport=0 flags=RA seq=2 win=0 rtt=16.7 ms

--- 10.33.107.39 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 12.8/14.2/16.7 ms
```

7. Perhatikan hasil tangkapan Wireshark di Windows.



Dari hasil tangkapan di atas, terdapat 1080967 paket yang terkirim.

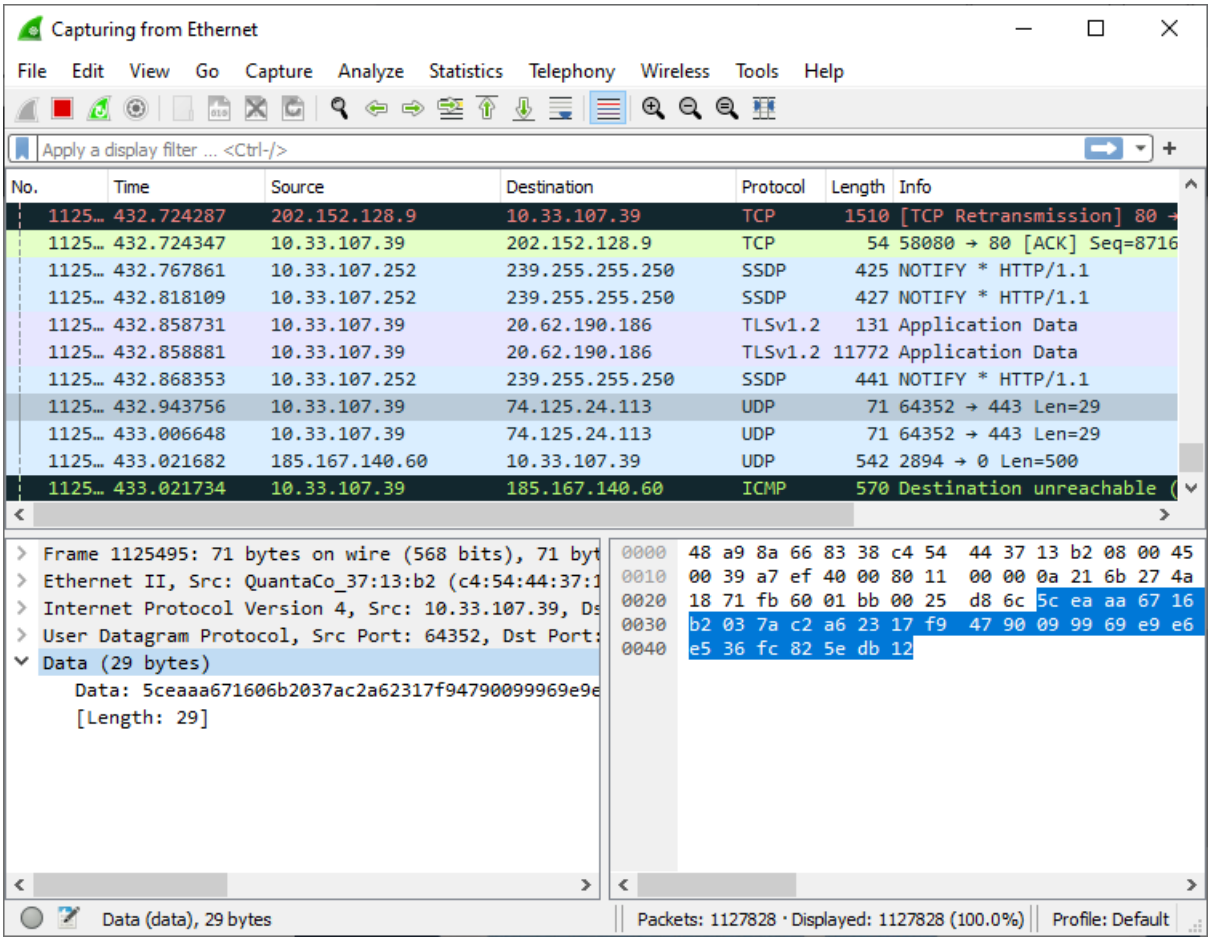
8. Ketik **hping3 –scan 1-3000 -S 10.33.107.39** (IP PC Windows) dan ketik *Enter*.

```
┌──(root💀kali)-[/home/kali]
└─# hping3 --scan 1-3000 -S 10.33.107.39
Scanning 10.33.107.39 (10.33.107.39), port 1-3000
3000 ports to scan, use -V to see all the replies
+----+------------+---------+---+-----+-----+-----+
|port| serv name  |  flags  |ttl| id  | win | len |
+----+------------+---------+---+-----+-----+-----+
  135 epmap      : .S..A... 127 13260 65392    46
  139 netbios-ssn: .S..A... 127 13516  8192    46
  445 microsoft-d: .S..A... 127 13772 65392    46
 1521            : .S..A... 127 47052 65392    46
 2031            : .S..A... 127 65484 65392    46
All replies received. Done.
Not responding ports: (565 ) (576 ) (582 ) (599 ) (602 ) (603 ) (709 ) (710 ) (711 ) (713 ) (714 ) (
(735 ) (747 ) (750 kerberos4) (789 ) (790 ) (811 ) (982 ) (983 ) (984 ) (986 ) (1024 ) (1033 ) (1034
) (1054 ) (1055 ) (1056 ) (1057 ) (1058 ) (1059 ) (1060 ) (1061 ) (1062 ) (1063 ) (1064 ) (1065 ) (1
78 ) (1079 ) (1080 socks) (1081 ) (1082 ) (1083 ) (1084 ) (1085 ) (1086 ) (1087 ) (1088 ) (1089 ) (1
(1385 ) (1386 ) (1388 ) (1390 ) (1405 ) (1406 ) (1407 ) (1408 ) (1409 ) (1410 ) (1411 ) (1412 ) (141
 ) (1476 ) (1477 ) (1478 ) (1479 ) (1480 ) (1481 ) (1482 ) (1483 ) (1484 ) (1485 ) (1486 ) (1487 ) (
557 ) (1563 ) (1565 ) (1567 ) (1568 ) (1569 ) (1570 ) (1572 ) (1573 ) (1575 ) (1577 ) (1579 ) (1580
 (1736 ) (1760 ) (1761 ) (1762 ) (1763 ) (1764 ) (1765 ) (1766 ) (1772 ) (1773 ) (1774 ) (1777 ) (17
0 ) (1851 ) (1852 ) (1853 ) (1854 ) (1855 ) (1856 ) (1857 ) (1858 ) (1859 ) (1861 ) (1863 ) (1864 )
1884 ) (1885 ) (1888 ) (1990 ) (2010 ) (2021 ) (2079 ) (2251 ) (2252 ) (2253 ) (2256 ) (2257 ) (2259
) (2290 ) (2293 ) (2298 ) (2299 ) (2300 ) (2304 ) (2308 ) (2309 ) (2310 ) (2311 ) (2312 ) (2313 ) (2
26 ) (2327 ) (2340 ) (2427 ) (2428 ) (2429 ) (2430 venus) (2431 venus-se) (2433 codasrv-se) (2434 )
6 ) (2747 ) (2748 ) (2749 ) (2750 ) (2751 ) (2752 ) (2753 ) (2754 ) (2755 ) (2756 ) (2757 ) (2758 )
2821 ) (2822 ) (2823 ) (2824 ) (2825 ) (2826 ) (2827 ) (2828 ) (2829 ) (2830 ) (2831 ) (2832 ) (2833
) (2847 ) (2848 ) (2849 ) (2850 ) (2851 ) (2852 ) (2853 ) (2904 ) (2905 ) (2908 ) (2910 ) (2913 ) (2
71 ) (2977 ) (2980 ) (2981 ) (2992 ) (2994 ) (2995 ) (2996 ) (2997 ) (2998 ) (2999 ) (3000 )
```

9. Untuk melakukan pembuatan paket UDP, ketik **hping3 10.33.107.39 –udp –rand-source –data 500** dan tekan *Enter*.

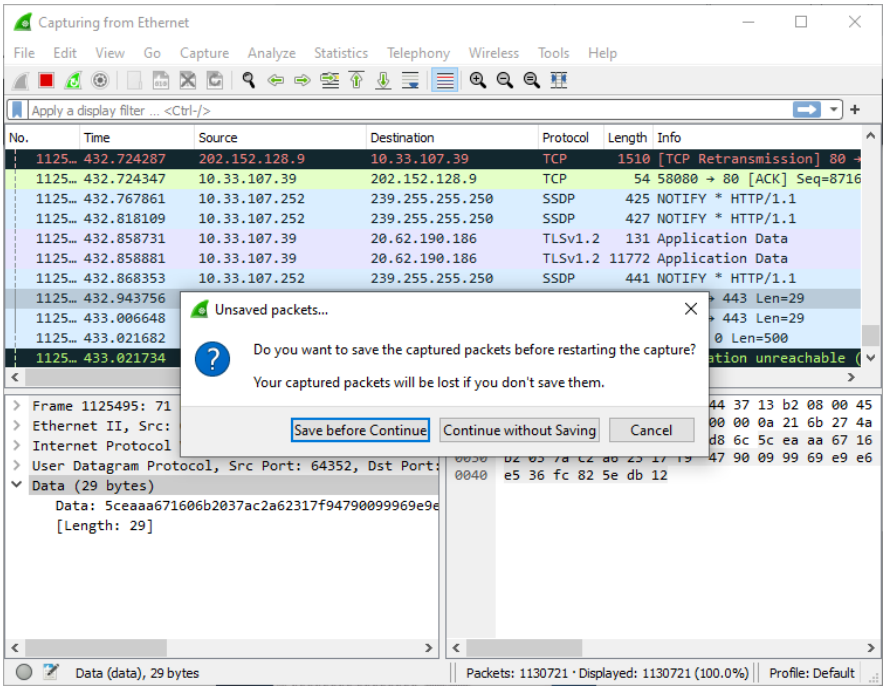
```
┌──(root💀kali)-[/home/kali]
└─# hping3 10.33.107.39 --udp --rand-source --data 500
HPING 10.33.107.39 (eth0 10.33.107.39): udp mode set, 28 headers + 500 data bytes
```

10. Beralih ke mesin Windows dan klik paket UDP apa pun untuk melihat detail paket. Di panel detail paket, perluas bagian Data untuk melihat ukuran data paket.



Dari tampilan di atas, ukuran data paket adalah 29 *bytes.*

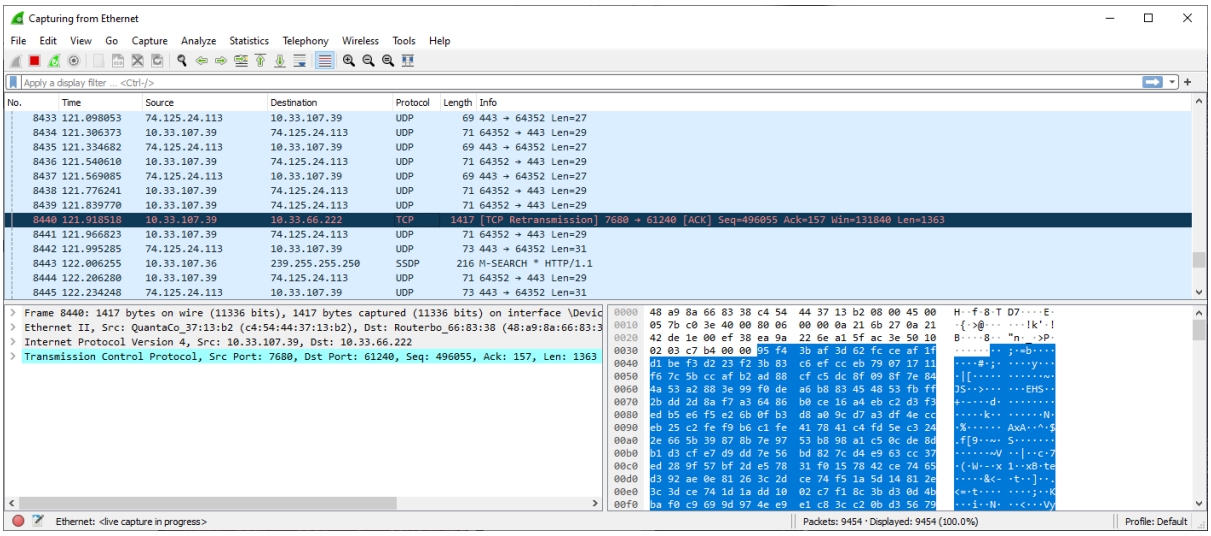
11. Klik tombol *Restart Packet Capturing* dari bilah menu dan klik *Continue Without Saving* tombol masuk *Unsaved packets*…



12. Kirim permintaan TCP SYN ke mesin target, ketik **hping3 -S 10.33.107.39 -p 80 -c 5** dan tekan *Enter*.

```
┌──(root💀kali)-[/home/kali]
└─# hping3 -S 10.33.107.39 -p 80 -c 5
HPING 10.33.107.39 (eth0 10.33.107.39): S set, 40 headers + 0 data bytes
len=46 ip=10.33.107.39 ttl=127 DF id=58956 sport=80 flags=RA seq=0 win=0 rtt=11.9 ms
len=46 ip=10.33.107.39 ttl=127 DF id=59274 sport=80 flags=RA seq=1 win=0 rtt=11.9 ms
len=46 ip=10.33.107.39 ttl=127 DF id=59431 sport=80 flags=RA seq=2 win=0 rtt=11.7 ms
len=46 ip=10.33.107.39 ttl=127 DF id=59585 sport=80 flags=RA seq=3 win=0 rtt=15.5 ms
len=46 ip=10.33.107.39 ttl=127 DF id=59737 sport=80 flags=RA seq=4 win=0 rtt=15.3 ms

--- 10.33.107.39 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 11.7/13.3/15.5 ms
```

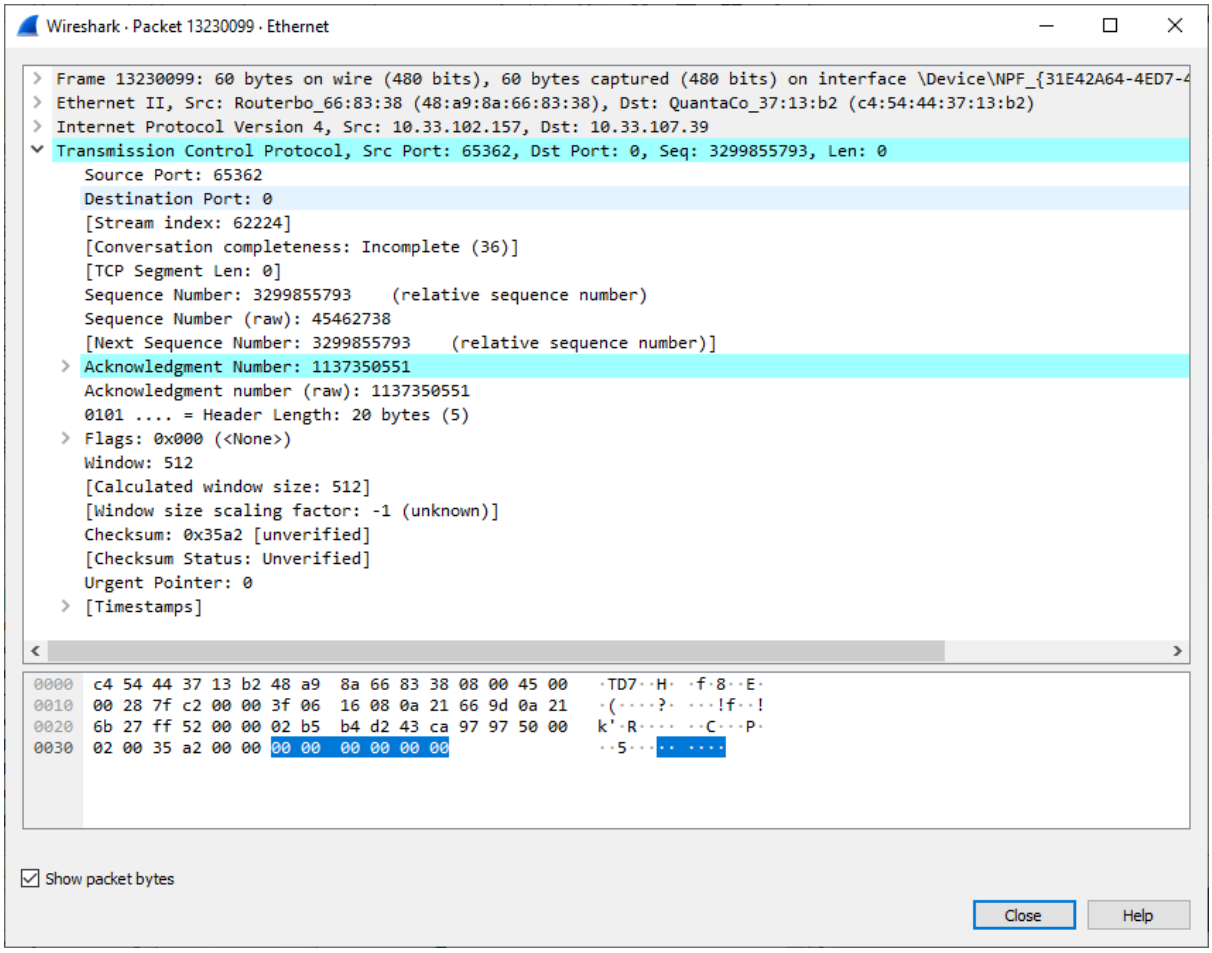
13. Sekarang beralih ke Windows 10 dan amati paket TCP pada Wireshark.



14. Beralih ke Kali Linux masuk ke *terminal* dan ketik **hping3 10.33.107.39 --flood** dan tekan *Enter*.

```
┌──(root💀kali)-[/home/kali]
└─# hping3 10.33.107.39 --flood
HPING 10.33.107.39 (eth0 10.33.107.39): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

15. Beralih ke Windows 10 dan amati Wireshark yang menampilkan paket TCP yang membanjiri dari mesin penyerang.
16. Klik dua kali paket TCP pada aliran paket untuk mengamati informasi paket TCP. Aliran Paket TCP menampilkan informasi lengkap paket TCP yang ditransmisikan ke mesin penyerang dan paket yang diterima.



B. *Reconnaissance*

1. dnsrecon -d www.acme.com

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -d www.acme.com
[*] Performing General Enumeration of Domain: www.acme.com
[-] DNSSEC is not configured for www.acme.com
[*]     NS dns1.name-services.com 64.98.148.137
[*]     NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*]     NS dns2.name-services.com 216.40.47.201
[*]     NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*]     NS dns5.name-services.com 64.98.148.139
[*]     NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*]     NS dns3.name-services.com 64.98.148.138
[*]     NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*]     NS dns4.name-services.com 216.40.47.202
[*]     NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[-] Could not Resolve MX Records for www.acme.com
[*]     CNAME www.acme.com acme.com
[*]     A acme.com 23.93.76.124
[*] Enumerating SRV Records
[+] 0 Records Found
```

2. dnsrecon -d www.certifiedhacker.com

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -d www.certifiedhacker.com
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
```

3. dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt
[-] Could not resolve NS server provided and server doesn't appear to be an IP: ns_server
[-] Please specify valid name servers.
```

4. dnsrecon -d www.acme.com -t zonewalk

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -d www.acme.com -t zonewalk
[*] Performing NSEC Zone Walk for www.acme.com
[*] Getting SOA record for www.acme.com
[-] This zone appears to be misconfigured, no SOA record found.
[*]      CNAME www.acme.com acme.com
[*]      A acme.com 23.93.76.124
[+] 2 records found
```

5. dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt
[-] File /path/to/dict.txt does not exist!
```

6. dnsrecon -d www.acme.com -t axfr

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -d www.acme.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for www.acme.com name servers
[*] Resolving SOA Record
[*] Resolving NS Records
[*] NS Servers found:
[*]      NS dns2.name-services.com 216.40.47.201
[*]      NS dns2.name-services.com 2604:4000:0:d:216:40:47:201
[*]      NS dns5.name-services.com 64.98.148.139
[*]      NS dns5.name-services.com 2604:4000:2800:2000:64:98:148:139
[*]      NS dns1.name-services.com 64.98.148.137
[*]      NS dns1.name-services.com 2604:4000:2800:2000:64:98:148:137
[*]      NS dns4.name-services.com 216.40.47.202
[*]      NS dns4.name-services.com 2604:4000:0:d:216:40:47:202
[*]      NS dns3.name-services.com 64.98.148.138
[*]      NS dns3.name-services.com 2604:4000:2800:2000:64:98:148:138
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:139
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:139!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:0:d:216:40:47:202
[-] Zone Transfer Failed for 2604:4000:0:d:216:40:47:202!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 216.40.47.201
[-] Zone Transfer Failed for 216.40.47.201!
[-] Port 53 TCP is being filtered
[*]
```

```
[*] Trying NS server 64.98.148.138
[-] Zone Transfer Failed for 64.98.148.138!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:0:d:216:40:47:201
[-] Zone Transfer Failed for 2604:4000:0:d:216:40:47:201!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.139
[-] Zone Transfer Failed for 64.98.148.139!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 64.98.148.137
[-] Zone Transfer Failed for 64.98.148.137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 216.40.47.202
[-] Zone Transfer Failed for 216.40.47.202!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:137
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:137!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2604:4000:2800:2000:64:98:148:138
[-] Zone Transfer Failed for 2604:4000:2800:2000:64:98:148:138!
[-] Port 53 TCP is being filtered
```

7. dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com

```
┌──(root💀kali)-[/home/kali]
└─# dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 208.67.222.200 to 208.67.222.255
[+] PTR resolver3.opendns.com 208.67.222.220
[+] PTR dns.umbrella.com 208.67.222.222
[+] PTR resolver1.opendns.com 208.67.222.222
[+] PTR dns.opendns.com 208.67.222.222
[+] 4 Records Found
```

V. Pembahasan

Pada praktikum kali ini, terbagi menjadi 2 praktikum yang berbeda yaitu *footprinting* dan *reconnaissance*. *Footprinting* yang dilakukan pada praktikum ini adalah teknik *crafting* UDP dan TCP *packet* menggunakan hping3. Alamat IP yang menjadi tujuan pada praktik ini yaitu alamat IP PC masing-masing dengan hasil *crafting* yang dapat dilihat detailnya pada Wireshark. Perintah pertama yaitu '**hping3 -c 3 10.33.107.39'.** Dengan menggunakan perintah ini, pengirim mengirimkan tiga paket ke alamat IP 10.33.107.39, yang mana setelah dicek pada Wireshark terdapat 1080967 paket yang terkirim.

Perintah kedua yaitu '**hping3 –scan 1-3000 -S 10.33.107.39'**. Dalam perintah ini, digunakan opsi '-scan' untuk melakukan pemindaian *port* TCP dari 1 hingga 3000 pada alamat IP 10.33.107.39. Opsi -S menandakan bahwa paket TCP SYN akan dikirimkan sebagai bagian dari pemindaian. Kemudian dilakukan pembuatan paket UDP dengan perintah '**hping3 10.33.107.39 –udp –rand-source –data 500'**. Dengan perintah ini, paket UDP yang dibuat dikirimkan ke alamat IP 10.33.107.39. Opsi –udp menandakan bahwa paket yang dibuat adalah paket UDP. Opsi –rand-source mengindikasikan bahwa alamat sumber dalam paket akan secara acak dipilih. Opsi –data

500 menunjukkan bahwa paket akan memiliki data sebesar 500 *byte*. Namun, dari tampilan yang terlihat dalam Wireshark, ukuran data paket yang sebenarnya adalah 29 *byte*.

Selanjutnya dilakukan pengiriman permintaan TCP SYN menggunakan perintah '**hping3 -S 10.33.107.39 -p 80 -c 5**'. Dari tampilan paket TCP pada Wireshark, dapat dilihat bahwa paket TCP memiliki *port* sumber: 7680 dan *port* tujuan: 61240. Selain itu, nomor urutan dari paket TCP (*sequence number*) adalah 496055 dan *acknowledgment number*-nya 157. Panjang data dalam paket TCP ini adalah 1363 *bytes*.

Terakhir, pada *footprinting* dilakukan serangan *flood* pada alamat IP 10.33.107.39 menggunakan perintah '**hping3 10.33.107.39 --flood**'. Banyak paket yang telah dikirim ke mesin target jika menurut opsi *Frame* pada Wireshark adalah paket memiliki ukuran 60 *byte* atau 480 *bit* ketika dikirim melalui jaringan. Lalu *interface* telah menangkap seluruh paket dengan ukuran 60 *byte* atau 480 *bit*.

Reconnaissance yang dilakukan pada praktikum ini adalah mengumpulkan informasi terkait DNS menggunakan **dnsrecon.** DNSRecon merupakan alat pengumpul informasi DNS (*Domain Name System*) yang digunakan untuk menganalisis dan mendapatkan informasi tentang pengaturan DNS suatu *domain*. Praktik ini digunakan pada beberapa kasus sebagai berikut.

1. **dnsrecon -d www.acme.com**: Perintah ini digunakan untuk melakukan pencarian informasi DNS pada *domain* www.acme.com. DNSRecon akan mencoba mengumpulkan informasi seperti alamat IP, *server* DNS, catatan MX (*Mail Exchange*), dan sebagainya.
2. **dnsrecon -d www.certifiedhacker.com**: Perintah ini memiliki fungsi yang sama dengan perintah sebelumnya, tetapi digunakan untuk melakukan pencarian informasi DNS pada *domain* www.certifiedhacker.com.
3. **dnsrecon -t snoop -n ns_server -d www.acme.com -D /path/to/dict.txt**: Perintah ini digunakan untuk melakukan pengujian DNS dengan menggunakan teknik "snoop". Opsi -n digunakan untuk menentukan *server* DNS yang akan digunakan, -d untuk menyebutkan *domain* yang dituju, dan -D untuk menentukan kamus tebakan (*dictionary*) yang digunakan.
4. **dnsrecon -d www.acme.com -t zonewalk**: Perintah ini digunakan untuk melakukan pemeriksaan zona pada *domain* www.acme.com. Pemeriksaan zona (*zonewalk*) adalah proses mengumpulkan informasi rekaman DNS secara bertahap dan sistematis dari zona DNS yang ditentukan.
5. **dnsrecon -d www.acme.com -D /path/to/dict.txt -t brt**: Perintah ini digunakan untuk melakukan *brute force* pada *subdomain domain* www.acme.com dengan menggunakan kamus tebakan (*dictionary*) yang ditentukan melalui opsi -D. Opsi -t brt digunakan untuk menentukan jenis teknik serangan *brute force*.
6. **dnsrecon -d www.acme.com -t axfr**: Perintah ini digunakan untuk melakukan transfer zona pada *domain* www.acme.com dengan menggunakan teknik "AXFR" (zonetransfer). Teknik ini memungkinkan pengambilan rekaman DNS secara lengkap dari *server* DNS yang memegang zona *domain*.
7. **dnsrecon -r 208.67.222.200-208.67.222.255 -d microsoft.com**: Perintah ini digunakan untuk melakukan pencarian informasi DNS pada rentang alamat IP

208.67.222.200 hingga 208.67.222.255, untuk *domain* microsoft.com. Perintah ini memungkinkan pencarian informasi DNS pada rentang alamat IP yang ditentukan.

VI. Kesimpulan

1. Hping3 merupakan perintah yang digunakan untuk melakukan *crafting* pada UDP dan TCP *packet.*
2. Hasil *crafting* dapat dilihat pada Wireshark secara detail.
3. *Reconnaissance* adalah teknik untuk mengumpulkan informasi tentang target atau sistem yang akan diserang.
4. DNSRecon merupakan alat pengumpul informasi DNS (*Domain Name System*).

VII. Daftar Pustaka

McMillan, T. (2011). *Hacking Exposed 7: Network Security Secrets and Solutions*. McGraw-Hill Education.

Middleton, R., & Warren, K. (2012). *Hacking: The Next Generation*. O'Reilly Media.

Harris, S., & Harper, A. (2015). *Gray Hat Hacking: The Ethical Hacker's Handbook*. McGraw-Hill Education.

Beale, J., & Michael, J. T. (2015). *Mastering Modern Web Penetration Testing*. Packt Publishing.

EC-Council. (2017). *Certified Ethical Hacker (CEH) Version 9 Cert Guide (3rd ed.)*. Pearson IT Certification.

Patel, K., & Jangla, S. (2018). *Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 2019.2 - the ultimate white hat hackers' toolkit*. Packt Publishing.

Gordon, L. A., & Loeb, M. P. (2002). *The economics of information security investment. ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.