

DAFTAR PUSTAKA

- Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In *Cyber security and threats: Concepts, methodologies, tools, and applications* (pp. 608-621). IGI Global.
- Chonka, A., & Abawajy, J. (2012, September). Detecting and mitigating HX-DoS attacks against cloud web services. In *2012 15th International Conference on Network-Based Information Systems* (pp. 429-434). IEEE.
- Diansyah, T. M., Faisal, I., & Siregar, D. (2023). Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, 4(1), 224-233.
- EC-Council. (2020). *Certified Network Defender (CND) Version 2*. International Council of E-Commerce Consultants (EC Council).
- Fahrina, Miftahul. (2023). *Vulnerability Assessment Dalam Analisis Keamanan WLAN Departemen Teknik Elektro FT-UH*. Universitas Hasanuddin
- FIRST. (n.d.). *CVSS v4.0 Specification Document*. Forum of Incident Response and Security Teams. Retrieved December 13, 2023, from <https://www.first.org/cvss/v4.0/specification-document>
- Gantsou, D. (2015). On the use of security analytics for attack detection in vehicular ad hoc networks. In *2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC)* (pp. 1-6). IEEE.
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), 1155-1175.
- Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika: Jurnal Sistem Komputer*, 11(1), 67-76.

- Hesar, A. D., & Attari, M. A. (2014, December). Simulating and analysis of cyber attacks on a BLPC network. In 2014 Smart Grid Conference (SGC) (pp. 1-6). IEEE.
- Hu, X., Jang, J., Stoecklin, M. P., Wang, T., Schales, D. L., Kirat, D., & Rao, J. R. (2016, June). BAYWATCH: robust beaconing detection to identify infected hosts in large-scale enterprise networks. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 479-490). IEEE.
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 3171-3189.
- Indre, I., & Lemnaru, C. (2016, September). Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things. In 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP) (pp. 175-182). IEEE.
- Jing, T., Li, J., & Xing, R. (2012, February). Research on malicious links detection system based on script text analysis. In 2012 14th International Conference on Advanced Communication Technology (ICACT) (pp. 439-442). IEEE.
- Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST special publication, 800(150).
- Kali Linux Tools. (n.d.). ettercap. Retrieved September 12, 2023, from <https://www.kali.org/tools/ettercap/>
- Kali Linux Tools. (n.d.). hping3. Retrieved September 12, 2023, from <https://www.kali.org/tools/hping3/>
- Kali Linux Tools. (n.d.). macchanger. Retrieved September 12, 2023, from <https://www.kali.org/tools/macchanger/>
- Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.




- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.
- Nmap. (n.d.). Nmap Security Scanner. Retrieved September 12, 2023, from <https://nmap.org/>
- Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, 10(2), 60-67.
- Putra, M.R., & Pembimbing Achmad Imam Kistijantoro, S. (2011). ANALISIS DAN PENCEGAHAN SERANGAN MAN IN THE MIDDLE (MiTM) PADA OTENTIFIKASI WEB PROXY JARINGAN KAMPUS ITB.
- Rachman, R. (2021). Analisis Keamanan Jaringan Wireless LAN (WLAN) Dengan Metode Penetration Testing Pada PT. PLN (Persero) Sektor Pengendalian Pembangunan Pekanbaru (Doctoral dissertation, Universitas Islam Riau).
- Riadi, I., Umar, R., & Busthomi, I. (2020). Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain. *Journal of Information Engineering and Educational Technology*.
- Ron, M. (2018, April). Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In *Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018)* (Vol. 94, p. 12). Springer.
- Salazar Soler, J. (2017). *Wireless networks*. Czech Technical University of Prague.
- Saputra, A. S., & Irwan, D. (2020). Sistem Keamanan Pada Jaringan Wireless Menggunakan Protokol RADIUS. *JUSS (Jurnal Sains dan Sistem Informasi)*, 3(2), 28-34.
- Telkom University. (n.d.). Kali Linux: Pengertian, Sejarah, Kelebihan, Kekurangan & Jenisnya. Retrieved September 12, 2023, from <https://it.telkomuniversity.ac.id/kali-linux-pengertian-sejarah-kelebihan-kekurangan-jenisnya/>

- Telkom University. (n.d.). Pengertian Sistem Operasi Windows: Sejarah, Fungsi, dan Fiturnya. Retrieved September 12, 2023, from <https://it.telkomuniversity.ac.id/pengertian-sistem-operasi-windows/>
- Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. *The Oxford handbook of international political theory*, 259.
- Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security—what goes where?. *Information & Computer Security*, 26(1), 2-9.
- Wireshark. (n.d.). Frequently Asked Questions. Retrieved September 12, 2023, from https://www.wireshark.org/faq.html#_what_is_wireshark
- Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of service attacks, defences and research challenges. *Cluster Computing*, 20, 661-671.

LAMPIRAN

Lampiran 1 *Login section* jaringan WLAN kampus

UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK

Informasi :

1. Untuk semua Pegawai teknik Unhas user dan password dapat diambil di Dekanat
2. Username dan password login dosen dan mahasiswa dapat diambil pada Lab Komputer B Gedung CSA Lt. 2, mahasiswa menyertakan kartu mahasiswa yang masih berlaku
3. Permintaan username dan password login hanya dilayani pada jam kerja kantor
4. Apabilan terdapat gangguan jaringan/koneksi ke internet, agar kiranya menghubungi tim teknis untuk melakukan troubleshooting
5. Apabilan lupa password login hotspot atau pembuatan login hotspot kiranya datang ke Lab Komputer B Gedung CSA Lt. 2
keluhan & saran : [klik disini](#)

Kontak Person Tim Teknis DSTI UNHAS :

- **Ryan~ +6285256183103**
- **Muhlis~ +6282396131054**
- **Janu~ +6282195188458**
- **Iam~ +6282190836810**

Lampiran 2 Trafik ping machine attacker ke machine victim

The image shows two windows from a Kali Linux system. The left window is a terminal where a ping command is being executed against the IP address 192.168.44.101. The output shows successful responses from 192.168.44.101 with varying times and TTL values. The right window is Wireshark, which is capturing network traffic on the wlan0 interface. The packet list pane shows a series of ICMP Echo (ping) replies from 192.168.42.68 to 192.168.44.101. The packet details pane shows the structure of an ICMP Echo (ping) reply, including the type, code, and data field.

```

kali@kali:~$ ping 192.168.44.101
PING 192.168.44.101 (192.168.44.101) 56(60) bytes of data:
64 bytes from 192.168.44.101: icmp_seq=1 ttl=128 time=8.46 ms
64 bytes from 192.168.44.101: icmp_seq=2 ttl=128 time=8.69 ms
64 bytes from 192.168.44.101: icmp_seq=3 ttl=128 time=130 ms
64 bytes from 192.168.44.101: icmp_seq=4 ttl=128 time=130 ms
64 bytes from 192.168.44.101: icmp_seq=5 ttl=128 time=16.8 ms
64 bytes from 192.168.44.101: icmp_seq=6 ttl=128 time=236 ms
64 bytes from 192.168.44.101: icmp_seq=7 ttl=128 time=12.4 ms
64 bytes from 192.168.44.101: icmp_seq=8 ttl=128 time=290 ms
64 bytes from 192.168.44.101: icmp_seq=9 ttl=128 time=12.6 ms
^C
--- 192.168.44.101 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8010ms
rtt min/avg/max/mdev = 8.464/124.586/398.318/140.817 ms
kali@kali:~$
  
```

Lampiran 3 Paket ICMP yang dikirim oleh machine attacker

The image shows a Wireshark capture of network traffic on the wlan0 interface. The packet list pane displays a large number of ICMP Echo (ping) replies from the source IP 192.168.42.68 to the destination IP 192.168.44.101. The packet details pane shows the structure of an ICMP Echo (ping) reply, including the type, code, and data field.

No.	Time	Source	Destination	Protocol	Length	Info
7025...	417.781502863	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.782552982	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.783310549	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.784506751	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.786331690	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.787215639	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.788760824	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.789799505	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.790940910	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.791757279	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.792758797	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.793667440	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.794895470	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.796674271	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.797625698	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.799279749	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.800438555	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.802403039	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.804234076	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.806540756	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.807451758	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.809579291	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.810579305	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.811617228	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.812699826	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.813633181	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.815636908	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.816541528	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.817649939	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.818611744	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.820001193	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.820985633	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.821938430	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.822922245	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.823806779	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.824818374	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.825961560	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.826896877	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.827716205	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.828778190	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.830310280	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.831198924	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.833106560	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.834116923	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.835150844	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.836207561	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.837024246	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...
7025...	417.838134325	192.168.42.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0x...

Lampiran 4 Paket ICMP yang diterima oleh *machine victim*

The screenshot shows a Wireshark capture of ICMP traffic. The main pane displays a list of 24 ICMP Echo (ping) replies and one Echo (ping) request. All packets are from source IP 192.168.41.229 to destination IP 192.168.42.68. The 'Info' column shows details such as 'Echo (ping) reply' and 'request in' followed by a sequence number and TTL. The bottom pane shows the packet details for frame 401, indicating it is an Echo (ping) request with a TTL of 64 and no response found.

No.	Time	Source	Destination	Protocol	Length	Info
L 5157..	414.199594	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=47975/26555, ttl=128 (request in 515517)
L 5157..	414.199629	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=48231/26556, ttl=128 (request in 515518)
L 5157..	414.199665	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=48487/26557, ttl=128 (request in 515519)
L 5158..	414.199700	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=48743/26558, ttl=128 (request in 515520)
L 5158..	414.199735	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=48999/26559, ttl=128 (request in 515521)
L 5158..	414.199771	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=49255/26560, ttl=128 (request in 515522)
L 5158..	414.199806	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=49511/26561, ttl=128 (request in 515523)
L 5158..	414.199841	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=49767/26562, ttl=128 (request in 515524)
L 5158..	414.199877	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=50023/26563, ttl=128 (request in 515525)
L 5158..	414.199912	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=51303/26568, ttl=128 (request in 515526)
L 5158..	414.199948	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=51559/26569, ttl=128 (request in 515527)
L 5158..	414.199987	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=51815/26570, ttl=128 (request in 515528)
L 5158..	414.200024	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=52071/26571, ttl=128 (request in 515529)
L 5158..	414.200060	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=52327/26572, ttl=128 (request in 515530)
L 5158..	414.200098	192.168.41.229	192.168.42.68	ICMP	42	Echo (ping) reply id=0xc859, seq=52583/26573, ttl=128 (request in 515531)
L 5158..	414.43222	192.168.41.229	192.168.41.229	ICMP	42	Echo (ping) request id=0xc859, seq=52839/26574, ttl=64 (no response found!)

Lampiran 5 Paket TCP yang dikirim oleh *machine attacker*

The screenshot shows a Wireshark capture of TCP traffic. The main pane displays a list of 100 TCP RST (Reset) packets. All packets are from source IP 380 to destination IP 192.168.41.229. The 'Info' column shows details such as '[RST, ACK] Seq=1' followed by a sequence number. The bottom pane shows the packet details for frame 267061, indicating it is a TCP RST packet with a sequence number of 1 and an acknowledgment number of 65.

No.	Time	Source	Destination	Protocol	Length	Info
2933..	380.851446744	192.168.41.229	192.168.41.229	TCP	54	0 - 55606 [RST, ACK] Seq=1
2933..	380.852374194	192.168.41.229	192.168.41.229	TCP	54	0 - 56040 [RST, ACK] Seq=1
2933..	380.854162522	192.168.41.229	192.168.41.229	TCP	54	0 - 56939 [RST, ACK] Seq=1
2933..	380.854939403	192.168.41.229	192.168.41.229	TCP	54	0 - 57348 [RST, ACK] Seq=1
2933..	380.855917528	192.168.41.229	192.168.41.229	TCP	54	0 - 57866 [RST, ACK] Seq=1
2933..	380.856820422	192.168.41.229	192.168.41.229	TCP	54	0 - 58342 [RST, ACK] Seq=1
2934..	380.858490213	192.168.41.229	192.168.41.229	TCP	54	0 - 59082 [RST, ACK] Seq=1
2934..	380.859133009	192.168.41.229	192.168.41.229	TCP	54	0 - 59406 [RST, ACK] Seq=1
2934..	380.860077928	192.168.41.229	192.168.41.229	TCP	54	0 - 59939 [RST, ACK] Seq=1
2934..	380.861504866	192.168.41.229	192.168.41.229	TCP	54	0 - 60636 [RST, ACK] Seq=1
2934..	380.862335306	192.168.41.229	192.168.41.229	TCP	54	0 - 61025 [RST, ACK] Seq=1
2934..	380.863344212	192.168.41.229	192.168.41.229	TCP	54	0 - 61553 [RST, ACK] Seq=1
2934..	380.864378959	192.168.41.229	192.168.41.229	TCP	54	0 - 62152 [RST, ACK] Seq=1
2934..	380.865582697	192.168.41.229	192.168.41.229	TCP	54	0 - 62803 [RST, ACK] Seq=1
2934..	380.866580488	192.168.41.229	192.168.41.229	TCP	54	0 - 63287 [RST, ACK] Seq=1
2934..	380.867672879	192.168.41.229	192.168.41.229	TCP	54	0 - 63620 [RST, ACK] Seq=1
2934..	380.868301812	192.168.41.229	192.168.41.229	TCP	54	0 - 63921 [RST, ACK] Seq=1
2934..	380.869402189	192.168.41.229	192.168.41.229	TCP	54	0 - 64462 [RST, ACK] Seq=1
2934..	380.871417966	192.168.41.229	192.168.41.229	TCP	54	0 - 65346 [RST, ACK] Seq=1
2934..	380.872067759	192.168.41.229	192.168.41.229	TCP	54	0 - 125 [RST, ACK] Seq=1
2934..	380.873144146	192.168.41.229	192.168.41.229	TCP	54	0 - 693 [RST, ACK] Seq=1
2934..	380.876320196	192.168.41.229	192.168.41.229	TCP	54	0 - 1619 [RST, ACK] Seq=1
2934..	380.876342536	192.168.41.229	192.168.41.229	TCP	54	0 - 1620 [RST, ACK] Seq=1
2934..	380.876739667	192.168.41.229	192.168.41.229	TCP	54	0 - 1766 [RST, ACK] Seq=1
2934..	380.877927955	192.168.41.229	192.168.41.229	TCP	54	0 - 2269 [RST, ACK] Seq=1
2934..	380.878688378	192.168.41.229	192.168.41.229	TCP	54	0 - 2678 [RST, ACK] Seq=1
2934..	380.879761418	192.168.41.229	192.168.41.229	TCP	54	0 - 3205 [RST, ACK] Seq=1
2934..	380.883056778	192.168.41.229	192.168.41.229	TCP	54	0 - 4163 [RST, ACK] Seq=1
2934..	380.883062538	192.168.41.229	192.168.41.229	TCP	54	0 - 4164 [RST, ACK] Seq=1
2934..	380.883427411	192.168.41.229	192.168.41.229	TCP	54	0 - 4279 [RST, ACK] Seq=1
2934..	380.885179058	192.168.41.229	192.168.41.229	TCP	54	0 - 5181 [RST, ACK] Seq=1
2934..	380.886457754	192.168.41.229	192.168.41.229	TCP	54	0 - 5599 [RST, ACK] Seq=1
2934..	380.888063864	192.168.41.229	192.168.41.229	TCP	54	0 - 6539 [RST, ACK] Seq=1
2934..	380.890498749	192.168.41.229	192.168.41.229	TCP	54	0 - 7674 [RST, ACK] Seq=1
2934..	380.891174665	192.168.41.229	192.168.41.229	TCP	54	0 - 8095 [RST, ACK] Seq=1
2934..	380.892202771	192.168.41.229	192.168.41.229	TCP	54	0 - 8592 [RST, ACK] Seq=1
2934..	380.893507754	192.168.41.229	192.168.41.229	TCP	54	0 - 9179 [RST, ACK] Seq=1
2934..	380.894268631	192.168.41.229	192.168.41.229	TCP	54	0 - 9527 [RST, ACK] Seq=1
2934..	380.895250902	192.168.41.229	192.168.41.229	TCP	54	0 - 10089 [RST, ACK] Seq=1
2934..	380.896308384	192.168.41.229	192.168.41.229	TCP	54	0 - 10681 [RST, ACK] Seq=1
2934..	380.898906952	192.168.41.229	192.168.41.229	TCP	54	0 - 11049 [RST, ACK] Seq=1
2934..	380.899270715	192.168.41.229	192.168.41.229	TCP	54	0 - 12039 [RST, ACK] Seq=1
2934..	380.900279308	192.168.41.229	192.168.41.229	TCP	54	0 - 12613 [RST, ACK] Seq=1
2934..	380.901509816	192.168.41.229	192.168.41.229	TCP	54	0 - 13173 [RST, ACK] Seq=1
2934..	380.902890680	192.168.41.229	192.168.41.229	TCP	54	0 - 13642 [RST, ACK] Seq=1
2934..	380.903624256	192.168.41.229	192.168.41.229	TCP	54	0 - 14000 [RST, ACK] Seq=1
2934..	380.904547071	192.168.41.229	192.168.41.229	TCP	54	0 - 14434 [RST, ACK] Seq=1
2934..	380.905705670	192.168.41.229	192.168.41.229	TCP	54	0 - 14995 [RST, ACK] Seq=1

Lampiran 6 Paket TCP yang diterima pada *machine victim*

Wireshark interface showing a list of TCP packets. The packets are all RST (Reset) packets from various source IP addresses to the destination IP 192.168.41.229. The status bar at the bottom indicates 353385 packets displayed, with 353150 (99.9%) shown.

No.	Time	Source	Destination	Protocol	Length	Info
3533...	449.047661	192.168.42.68	192.168.41.229	TCP	54	0 → 27139 [RST, ACK] Seq=1 Ack=3493272123 Win=0 Len=0
3533...	449.047661	192.168.42.68	192.168.41.229	TCP	54	0 → 61016 [RST, ACK] Seq=1 Ack=3690906971 Win=0 Len=0
3533...	449.048521	192.168.42.68	192.168.41.229	TCP	54	0 → 61584 [RST, ACK] Seq=1 Ack=1191450063 Win=0 Len=0
3533...	449.051962	192.168.42.68	192.168.41.229	TCP	54	0 → 62914 [RST, ACK] Seq=1 Ack=768661790 Win=0 Len=0
3533...	449.051962	192.168.42.68	192.168.41.229	TCP	54	0 → 63277 [RST, ACK] Seq=1 Ack=300000311 Win=0 Len=0
3533...	449.051962	192.168.42.68	192.168.41.229	TCP	54	0 → 63720 [RST, ACK] Seq=1 Ack=4259300040 Win=0 Len=0
3533...	449.052328	192.168.42.68	192.168.41.229	TCP	54	0 → 28477 [RST, ACK] Seq=1 Ack=3474602691 Win=0 Len=0
3533...	449.053009	192.168.42.68	192.168.41.229	TCP	54	0 → 24560 [RST, ACK] Seq=1 Ack=3275358119 Win=0 Len=0
3533...	449.055158	192.168.42.68	192.168.41.229	TCP	54	0 → 23992 [RST, ACK] Seq=1 Ack=3178847549 Win=0 Len=0
3533...	449.055586	192.168.42.68	192.168.41.229	TCP	54	0 → 56715 [RST, ACK] Seq=1 Ack=3532713337 Win=0 Len=0
3533...	449.057262	192.168.42.68	192.168.41.229	TCP	54	0 → 64529 [RST, ACK] Seq=1 Ack=3315673799 Win=0 Len=0
3533...	449.058437	192.168.42.68	192.168.41.229	TCP	54	0 → 65092 [RST, ACK] Seq=1 Ack=3818701262 Win=0 Len=0
3533...	449.063277	192.168.42.68	192.168.41.229	TCP	54	0 → 95 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3533...	449.063277	192.168.42.68	192.168.41.229	TCP	54	0 → 890 [RST, ACK] Seq=1 Ack=60785357 Win=0 Len=0
3533...	449.063277	192.168.42.68	192.168.41.229	TCP	54	0 → 1203 [RST, ACK] Seq=1 Ack=3813954096 Win=0 Len=0
3533...	449.067172	192.168.42.68	192.168.41.229	TCP	54	0 → 2045 [RST, ACK] Seq=1 Ack=17649418 Win=0 Len=0

Frame 11807: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface v...
 Ethernet II, Src: TP-Link_S1:ee:ed (30:de:4b:51:ee:ed), Dst: IntelCor_e5:ab:69 (58:ce:20:29:e5:00)
 Internet Protocol Version 4, Src: 192.168.42.68, Dst: 192.168.41.229
 Transmission Control Protocol, Src Port: 0, Dst Port: 57562, Seq: 1, Ack: 1330715077

Lampiran 7 Paket UDP yang dikirim oleh *machine attacker*

Wireshark interface showing a list of UDP packets. The packets are all sent to the destination IP 192.168.41.229. The status bar at the bottom indicates 357932 packets displayed, with 357860 (100.0%) shown.

No.	Time	Source	Destination	Protocol	Length	Info
3578...	535.322484339	192.168.42.68	192.168.41.229	UDP	42	33091 → 0 Len=0
3578...	535.322486149	192.168.42.68	192.168.41.229	UDP	42	33092 → 0 Len=0
3578...	535.322488271	192.168.42.68	192.168.41.229	UDP	42	33093 → 0 Len=0
3578...	535.322490053	192.168.42.68	192.168.41.229	UDP	42	33094 → 0 Len=0
3578...	535.322491676	192.168.42.68	192.168.41.229	UDP	42	33095 → 0 Len=0
3578...	535.322493631	192.168.42.68	192.168.41.229	UDP	42	33096 → 0 Len=0
3578...	535.322495491	192.168.42.68	192.168.41.229	UDP	42	33097 → 0 Len=0
3578...	535.322497183	192.168.42.68	192.168.41.229	UDP	42	33098 → 0 Len=0
3578...	535.322498744	192.168.42.68	192.168.41.229	UDP	42	33099 → 0 Len=0
3578...	535.322500692	192.168.42.68	192.168.41.229	UDP	42	33100 → 0 Len=0
3578...	535.322503215	192.168.42.68	192.168.41.229	UDP	42	33101 → 0 Len=0
3578...	535.322505146	192.168.42.68	192.168.41.229	UDP	42	33102 → 0 Len=0
3578...	535.322508869	192.168.42.68	192.168.41.229	UDP	42	33103 → 0 Len=0
3578...	535.322510843	192.168.42.68	192.168.41.229	UDP	42	33104 → 0 Len=0
3578...	535.322513159	192.168.42.68	192.168.41.229	UDP	42	33105 → 0 Len=0
3579...	535.322515246	192.168.42.68	192.168.41.229	UDP	42	33106 → 0 Len=0
3579...	535.322516765	192.168.42.68	192.168.41.229	UDP	42	33107 → 0 Len=0
3579...	535.322518506	192.168.42.68	192.168.41.229	UDP	42	33108 → 0 Len=0
3579...	535.322520442	192.168.42.68	192.168.41.229	UDP	42	33109 → 0 Len=0
3579...	535.322522082	192.168.42.68	192.168.41.229	UDP	42	33110 → 0 Len=0
3579...	535.322523605	192.168.42.68	192.168.41.229	UDP	42	33111 → 0 Len=0
3579...	535.322525380	192.168.42.68	192.168.41.229	UDP	42	33112 → 0 Len=0
3579...	535.322527897	192.168.42.68	192.168.41.229	UDP	42	33113 → 0 Len=0
3579...	535.322530020	192.168.42.68	192.168.41.229	UDP	42	33114 → 0 Len=0
3579...	535.322531696	192.168.42.68	192.168.41.229	UDP	42	33115 → 0 Len=0
3579...	535.322533512	192.168.42.68	192.168.41.229	UDP	42	33116 → 0 Len=0
3579...	535.322535033	192.168.42.68	192.168.41.229	UDP	42	33117 → 0 Len=0
3579...	535.322536558	192.168.42.68	192.168.41.229	UDP	42	33118 → 0 Len=0
3579...	535.322538274	192.168.42.68	192.168.41.229	UDP	42	33119 → 0 Len=0
3579...	535.322539910	192.168.42.68	192.168.41.229	UDP	42	33120 → 0 Len=0
3579...	535.322541545	192.168.42.68	192.168.41.229	UDP	42	33121 → 0 Len=0
3579...	535.322543055	192.168.42.68	192.168.41.229	UDP	42	33122 → 0 Len=0
3579...	535.322545078	192.168.42.68	192.168.41.229	UDP	42	33123 → 0 Len=0
3579...	535.322547540	192.168.42.68	192.168.41.229	UDP	42	33124 → 0 Len=0
3579...	535.322549311	192.168.42.68	192.168.41.229	UDP	42	33125 → 0 Len=0
3579...	535.322550939	192.168.42.68	192.168.41.229	UDP	42	33126 → 0 Len=0
3579...	535.322552432	192.168.42.68	192.168.41.229	UDP	42	33127 → 0 Len=0
3579...	535.322554569	192.168.42.68	192.168.41.229	UDP	42	33128 → 0 Len=0
3579...	535.322556367	192.168.42.68	192.168.41.229	UDP	42	33129 → 0 Len=0
3579...	535.322558438	192.168.42.68	192.168.41.229	UDP	42	33130 → 0 Len=0
3579...	535.322560255	192.168.42.68	192.168.41.229	UDP	42	33131 → 0 Len=0
3579...	535.322561936	192.168.42.68	192.168.41.229	UDP	42	33132 → 0 Len=0
3579...	535.322563720	192.168.42.68	192.168.41.229	UDP	42	33133 → 0 Len=0
3579...	535.322565534	192.168.42.68	192.168.41.229	UDP	42	33134 → 0 Len=0
3579...	535.322567202	192.168.42.68	192.168.41.229	UDP	42	33135 → 0 Len=0
3579...	535.322568714	192.168.42.68	192.168.41.229	UDP	42	33136 → 0 Len=0
3579...	535.322574251	192.168.42.68	192.168.41.229	UDP	42	33137 → 0 Len=0
3579...	535.322575973	192.168.42.68	192.168.41.229	UDP	42	33138 → 0 Len=0

Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface v...
 Ethernet II, Src: TP-Link_S1:ee:ed (30:de:4b:51:ee:ed), Dst: IntelC...
 Internet Protocol Version 4, Src: 192.168.42.68, Dst: 192.168.41.229

Lampiran 8 Paket UDP yang diterima oleh *machine victim*

The screenshot shows a Wireshark capture of UDP traffic. The packet list pane displays 20 packets, all with source IP 192.168.42.68 and destination IP 192.168.41.229. The selected packet (No. 3796) is expanded to show the following details:

- Frame 256346: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
- Ethernet II, Src: TP-Link_S1:ee:red (30:de:4b:51:ee:red), Dst: IntelCon_e5:ab:69 (58:ce:2a:e5:ab:69)
- Internet Protocol Version 4, Src: 192.168.42.68, Dst: 192.168.41.229
- User Datagram Protocol, Src Port: 61994, Dst Port: 0

The packet bytes pane shows the raw data: 0000 58 ce 2a e5 ab 69 30 de 4b 51 ee ed 08 00 45 00 X * : : 10 KQ : : : E -

Lampiran 9 Trafik paket ARP yang diduplikasi dari *machine victim*

The screenshot shows a Wireshark capture of ARP traffic. The packet list pane displays a large number of packets, all with source MAC 30:de:4b:51:ee:red and destination MAC 30:de:4b:51:ee:red. The traffic is identified as ARP announcements. The list shows a high frequency of duplicate entries, such as:

- 56 Who has 192.168.42.68? Tell 192.168.40.100
- 42 ARP Announcement for 192.168.42.68
- 42 ARP Announcement for 192.168.40.122 (duplicate use of 192.168.40.122 detected!)

The traffic continues with many more similar entries, indicating a flood of duplicated ARP requests.