HASIL CEK_60020397_C67-Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology

by Imam Riadi 60020397

Submission date: 11-Dec-2020 11:00AM (UTC+0700)
Submission ID: 1471711949
File name: menggunakan_Metode_National_Institute_of_Standard_Technology.pdf (946.64K)
Word count: 2966
Character count: 18122

e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 4 No. 1, Juni, 2020, **Hal. 21-29**
DOI: 10.29408/edumatic.v4i1.2046

Analisis Bukti Serangan *Address Resolution Protocol Spoofing* menggunakan Metode *National Institute of Standard Technology*

Imam Riadi[1], Abdul Fadlil[2], Muhammad Nasir Hafizh[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
email: imam.riadi@is.uad.ac.id[1], fadlil@mti.uad.ac.id[2] ,m1907048019@webmail.uad.ac.id[3]

(Received: 19 April 2020/ Accepted: 6 Mei 2020 / Published Online: 20 Juni 2020)

Abstrak

Penelitian ini bertujuan untuk menemukan informasi bukti serangan *Address Resolution Protocol* (ARP) *Spoofing* berupa alamat MAC *address* penyerang dan korban beserta waktu terjadinya serangan. Penelitian ini menggunakan *tools* wireshark untuk melihat lalu lintas jaringan, terutama pada protokol ARP dan menggunakan metode *National Insitute of Standard Technology (NIST)* sebagai kerangka kerja selama proses simulasi sampai dengan pembuatan laporan barang bukti. Serangan ARP *Spoofing* dapat mengakibatkan terjadinya serangan lain, seperti *Denial of Service* dan *Man in The Middle Attack*, yanag mana serangan ini memungkinkan pengguna tidak dapat mengakses kedalam jaringan dan terjadinya pencurian data. Pada tahapan simulasi dilakukan 2 serangan ARP *Spoofing* terhadap 1 perangkat laptop dan 1 perangkat *routerboard* yang terhubung didalam jaringan. Hasil dari simulasi serangan berhasil ditemukan 2 serangan beserta informasi yang berhasil diperoleh, yaitu alamat MAC *address* penyerang dan korban beserta waktu terjadinya serangan. Berdasarkan hasil pengujian yang dilakukan, berhasil ditemukan semua serangan ARP *Spoofing* yang terjadi pada jaringan dengan tingkat keberhasilan 100%.

Kata kunci: *Address Resolution Protocol, National Institute of Standard Technology, Spoofing*

Abstract

This research intends to find information about evidence of Address Resolution Protocol (ARP) Spoofing attacks that is the MAC address of the attacker and victim also the time of the attack. This research uses Wireshark tools to inspect network traffic, especially on the ARP protocol. It uses the National Institute of Technology Technology (NIST) method as a framework in the simulation process to produce evidence reports. ARP Spoofing attacks can lead to other attacks, such as Denial of Service and Man in the Middle Attack, this attack allows users not to be able to access the network and data theft. During the simulation stage, 2 ARP Spoofing attacks are carried out on 1 laptop and 1 router connected to the network. The results of the attack simulation found 2 attacks and obtained information about the MAC address of the attacker and victim and also the time of the attack. Based on the results of tests carried, successfully found all ARP Spoofing attacks that occur on the network with a success rate of 100%

Keywords: *Address Resolution Protocol, NIST, Spoofing*

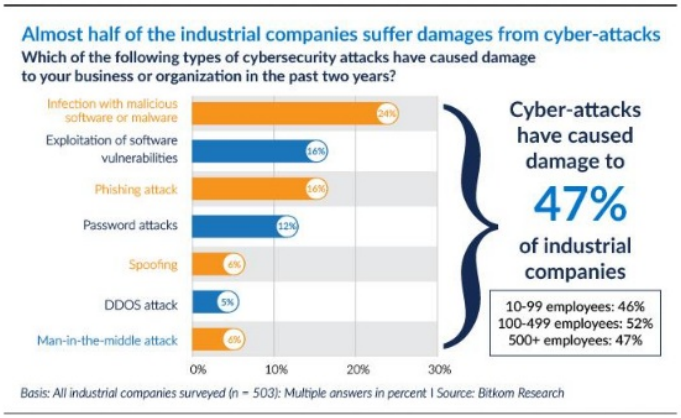
PENDAHULUAN

Pertumbuhan pengguna internet semakin meningkat. Meningkatnya pengguna internet tidak terlepas dari kemudahan yang didapatkan dalam menggunakan internet, seperti halnya dalam komunikasi jarak jauh tidak lagi menjadi kendala pada zaman sekarang ini, begitu juga didalam mengakses informasi, pengguna dapat dengan mudah memberikan dan mendapatkan informasi. Jaringan internet memberikan banyak kemudahan lain, sehingga membuat pengguna tidak menyadari adanya ancaman dari serangan siber pada jaringan komputer atau

internet. Indonesia (Jayani, 2019) statistik pengguna internet Indonesia diproyeksikan semakin meningkat setiap tahunnya seperti yang terlihat pada gambar 1.

Gambar 1. Statistik Pengguna Internet Indonesia

Pada gambar 1 dapat dilihat tahun 2018 data pengguna internet Indonesia sebanyak 95.2 juta tumbuh sebesar 13,3%. Pada tahun 2019 pengguna internet Indonesia diproyeksikan sebanyak 107,2 juta tumbuh sebesar 12.6%. Penelitian (Bitkom, 2018) menyatakan sebesar 47% dari perusahaan industri mengalami kerusakan dari serangan siber yang didominasi oleh serangan *malware* sebesar 24%. Hasil dari penelitian tersebut juga merilis serangan yang terjadi pada perusahaan industri, seperti yang terlihat pada gambar 2.



Gambar 2. Rangkuman Persentase Serangan Siber

Kasus yang terjadi pada perusahan industri seperti pencurian *email*, data pelanggan dan data keuangan. Serangan dengan metode *spoofing* juga merupakan salah satu serangan yang terjadi pada kasus kerusakan perusahaan industri diatas, dengan presentase serangan *spoofing* sebesar 6%.

Pada jaringan komputer terdapat *protocol* yang berfungsi sebagai penerjemah alamat IP *address* ke alamat MAC *address*, yang disebut *Address Resolution Protocol* (ARP), *Protocol* ARP bekerja dengan mengirimkan permintaan ARP secara *broadcast* untuk mencari alamat MAC *address* host yang dituju, metode pengiriman ARP secara *broadcast* ini merupakan celah sehingga dimanfaatkan oleh penyerang untuk memalsukan alamat MAC *address* host yang dituju. (Susianto, 2015). Penelitian yang dilakukan oleh (Veny Charnita Br Ginting, Mahendra Data, 2019) ARP *Spoofing* merupakan kejahatan siber atau serangan yang terjadi pada jaringan komputer dengan cara memalsukan alamat MAC *address* penerima. Peneliti melakukan pemerikasaan paket ARP dengan sebuah detektor host. Hasil dari penelitian ini merupakan akurasi presentase deteksi sebesar 89,64% dan waktu rata-rata deteksi adalah 0.4 detik. Penelitian juga dilakukan oleh (Kamajaya et al., 2020) dengan judul Analisa Investigasi Static Forensics Serangan Man In The Middle Berbasis ARP *Poisoning*, Hasil dari penelitian ini untuk menemukan data dan menemukan barang bukti.

Penelitian forensik jaringan telah dilakukan juga untuk mendeteksi *flooding attack* pada *web server* (Mualfah & Riadi, 2017). Pada penelitian tersebut, peneliti menerapkan sistem pendeteksi *Intrusion Detection System* (IDS) seperti *snort* yang merupakan sebuah *tools* digunakan untuk mendeteksi *flooding attack*. Semua aktifitas lalu lintas jaringan, nantinya akan tersimpan didalam *log file*, kemudian akan dilakukan analisis atau investigasi terhadap *log file* tersebut.

Forensik jaringan adalah ilmu yang berfokus pada jaringan komputer dan perangkat yang terhubung didalamnya, dalam upaya untuk menemukan informasi penyerang dan untuk mencari bukti atas serangan (Mazdadi et al., 2017). Menurut Rizal et al. (2018) Network Forensics merupakan proses mengambil, merekam serta menganalisis kegiatan pada lalu lintas jaringan untuk menemukan sumber serangan atau masalah lainnya. Pengambilan barang bukti pada *digital forensic* dapat dilakukan dengan cara *dead forensic* dan *live forensic*.(Yuwono et al., 2019). *Dead forensic* mengambil bukti digital yang tersimpan dimedia penyimpanan seperti *log file*, sedangkan live forensic mengambil bukti digital disaat *system* sedang menyala.

Penelitian dengan metode *live forensic* dilakukan oleh (Riadi, et al., 2018) dengan judul Identifikasi Bukti Digital WhatsApp pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*, penelitian ini menghasilkan barang bukti terkait kasus penipuan online dengan menggunakan *tool* ftk *imager*. Peneliti mengambil dan menganalisis data pada RAM, berupa percakapan WhatsApp (Riadi et al., 2019)

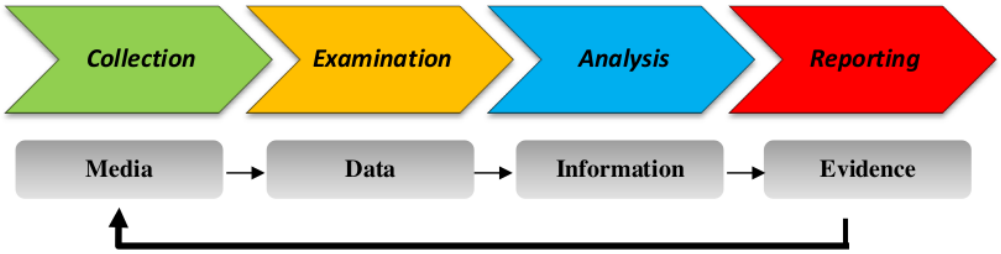
Kerangka kerja dalam penyusunan laporan investigasi suatu kasus dapat dilakukan dengan beberapa metode, diantaranya menggunakan metode *National Institute of Justice* (NIJ) dan *National Institute of Standard Technology* (NIST). Penelitian dengan metode NIJ dilakukan oleh (Riadi et al., n.d.) dengan judul Review Proses Forensik *Optical Drive* Menggunakan *Metode National Institute of Justice* (NIJ), penelitian ini mengembalikan hasil dari file yang telah diformat dengan menggunakan *tool* autopsy, untuk mendapatkan bukti digital. Penelitian dengan metode *National Institute of Standard Technology* dilakukan oleh (Riadi, Yudhana, et al., 2017) dengan judul Analisis *Recovery* Bukti Digital Instagram *Messangers* Menggunakan Metode *National Institute Of Standards And Technology* (NIST), hasil yang dari penelitian ini diharapkan mendapatkan barang bukti gambar dan pesan yang telah dihapus dengan menggunakan *tool recovery*.(Riadi, Yudhana, et al., 2018). Penelitian dengan menggunakan metode NIST juga dilakukan oleh (Syahib et al., 2020) dengan judul Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode *National Institute of Standards Technology* (NIST), dalam penelitian ini data yang berhasil didapatkan antar lain, akun pelaku, daftar kontak, riwayat panggilan, teks percakapan, dan pesan gambar/video. Metode NIST juga dilakukan oleh (Riadi, Umar, et al., 2017) hasil penelitian diperoleh rekaman percakapan, BBM *Identification Number* (BBM PIN), nama pengirim dan penerima, dan

waktu percakapan. Penelitian mengenai serangan *Distrbuted Denial of Service* dilakukan oleh(Aji et al., 2017) dengan judul Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan, penelitian tersebut mengenai serangan *Distributed Denial of Service*, yang menghasilkan data penyerang, dan waktu terjadinya serangan. (Fadlil et al., 2017)

Berdasarkan paparan masalah diatas, penelitian mengenai serangan ARP *Spoofing* dilakukan untuk mengidentifikasi penyerang dan korban sehingga admin jaringan dapat meningkatkan keamanan pada jaringan. Penelitian ini bertujuan untuk menemukan informasi bukti serangan *Address Resolution Protocol* (ARP) *Spoofing* berupa alamat MAC *address* penyerang dan korban beserta waktu terjadinya serangan.

METODE

Metode yang digunakan dalam penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) yang merupakan metode dalam menganalisis bukti digital. Metode NIST memiliki beberapa tahapan dalam proses analisis bukti digital, seperti yang terdapat pada gambar 3 (Riadi, Yudhana, et al., 2017).



Gambar 3. NIST Alur Proses

Pada gambar 2 dapat dilihat tahapan –tahapan pada proses analisis bukti digital :

1. *Collection*
   Tahap koleksi melakukan pengumpulan data, baik data literasi maupun data *real* simulasi. Pada tahap ini dilakukan identifikasi dan pengumpulan data dari proses simulasi dengan cara melakukan scanning pada jaringan.
2. *Examinatain*
   Tahap examination merupakan tahap pemeriksaan terhadap data yang diperoleh dari hasil scanning pada jaringan, terutama pada *protocol* ARP.
3. *Analysis*
   Tahap Analisis melakukan analisis dari hasil pemeriksaan dengan menggunakan metode legal dan dibenarkan untuk mendapatkan informasi yang berguna dan dijadikan jawaban dari pertanyaan yang dapat mendorong pengumpulan dan pemeriksaan.
4. *Reporting*
   Tahap pelaporan merupakan tahap melaporkan hasil analisis, yang meliputi jenis serangan, alamat IP *address* pelaku dan korban, alamat MAC *address* pelaku dan korban, serta waktu terjadinya serangan.

Penelitian ini menggunakan alat dan bahan berupa *hardware* dan *software* yang digunakan saat proses simulasi dan pengambilan data.

Tabel 1. Alat dan Bahan Penelitian

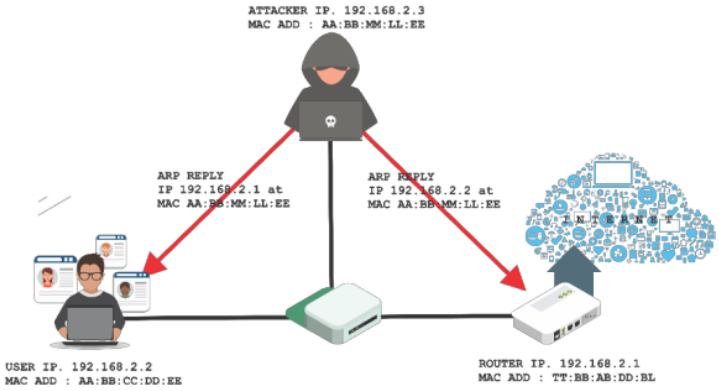
Hardware dan *Software*	Keterangan
Samsung Notebook NF210	Sebagai komputer yang digunakan untuk melakukan serangan ARP *spoofing*
ASUS Notebook A456U	Sebagai komputer yang digunakan sebagai investigator
Mikrotik Routerboard	Smart router yang digunakan untuk menghubungkan jaringan dengan internet
Wireshark	*Network Protocol Tool Analyzer*, *tool* yang digunakan untuk menganalisa lalu lintas paket pada jaringan
Ettercap	*Tool* yang digunakan untuk *melakukan* serangan arp *spoofing*

Pada tabel 2 disebutkan beberapa alat dan bahan yang digunakan dalam penelitian berupa *hardware* dan *software*. Alat dan bahan ini dikonfigurasi kedalam jaringan sesuai dengan topologi untuk memulai simulasi.

HASIL DAN PEMBAHASAN

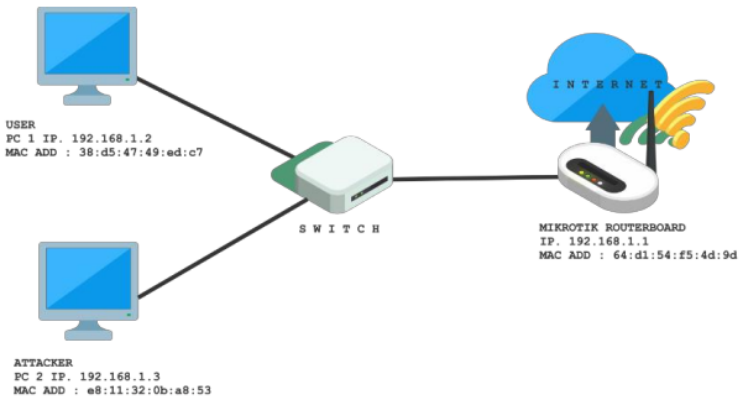
Collection (Pengumpulan Data)

Pada tahap ini dilakukan pengumpulan data dari literasi. Pengumpulan data juga dilakukan dengan melakukan simulasi seragan ARP *Spoofing* dengan cara melakukan scanning lalu lintas jaringan menggunakan *tools* wireshark. ARP *Spoofing* menyerang dengan memanipulasi alamat MAC *address* perangkat yang terhubung didalam jaringan, sehingga yang dikirim oleh host akan terlebih dahulu menuju kepada alamat MAC *address* penyerang. Isustrasi menegani serangan ARP Spoofing dapat dilihat pada gambar 4.



Gambar 4. Ilustrasi Serangan ARP *Spoofing*

Pada gambar 4 dapat dilihat, *attacker* mengirimkan ARP *reply* kepada *user* dan *router* untuk memanipulasi alamat MAC address penerima, sehingga paket yang dikirim akan melewati alamat MAC address *attacker*. Simulasi dan perangkat yang terhubung didalam jaringan dibuat sesuai dengan topologi yang digunakan dalam penelitian ini, topologi yang digunakan dalam jaringan in dapat dilihat pada gambar 5.



Gambar 5. Topologi Simulasi Pengambilan Data

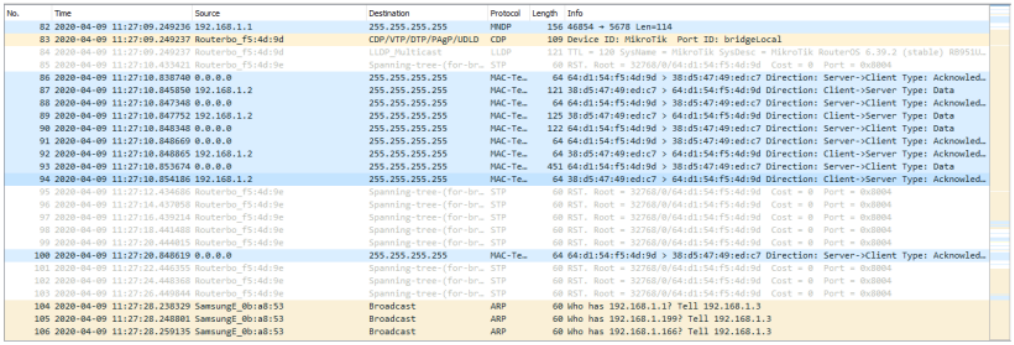
Pada gambar 5 diatas dapat dilihat perangkat yang terhubung dalam topologi jaringan yang digunakan dalam simulasi dalam kaitannya untuk mendapatkan informasi mengenai serangan ARP *Spoofing*. Pada tabel 2 dipaparkan pengaturan alamat IP address pada tiap perangkat dan informasi alamat MAC address pada tipa perangkat.

Tabel 2. Tabel Identitas Perangkat

Perangkat	*Ip Address*	MAC *Address*	Keterangan
Routerboard Mikrotik	192.168.1.1	64:d1:54:f5:4d:9d	Sebagai *router* dan *gateway*
PC 1 ASUS Notebook A456U	192.168.1.2	38:d5:47:49:ed:c7	Sebagai PC *Client* dengan *system* operasi *Windows* 10
PC 2 Samsung Notebook	192.168.1.3	e8:11:32:0b:a8:53	Sebagai PC *Attacker* dengan system operasi Kali Linux

Examintation (Pemerikasaan Data)

Pada tahapan ini dilakukan pengumpulan data dari serangan simulasi yang dibuat. Pengumpulan data dilakukan dengan melakukan scanning pada jaringan dengan menggunakan wireshark. Terdiri dari beberapa protocol yang berhasil didapat, Pada gambar 6 terlihat lalu lintas paket data dan protokol yang berhasil didapatkan. Protokol yang berhasil didapat antara lain *Spanning Tree Protocol* (STP), *Cisco Discovery Protocol* (CDP) dan *Address Resolution Protocol* (ARP).

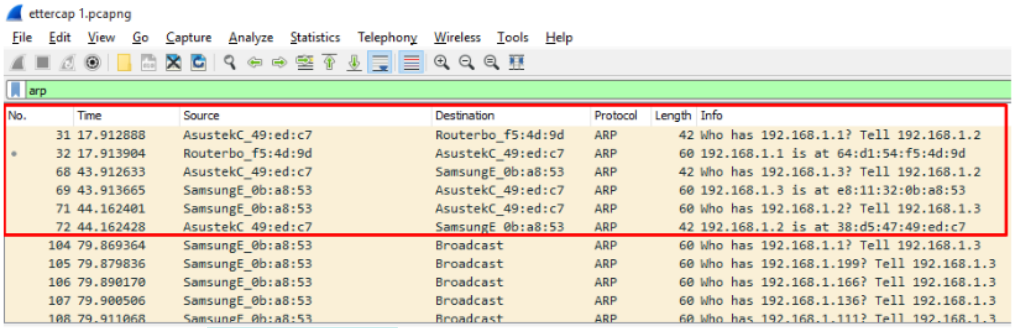


No.	Time	Source	Destination	Protocol	Length	Info
82	2020-04-09 11:27:09.249236	192.168.1.1	255.255.255.255	MNDP	156	46854 → 5678 Len=114
83	2020-04-09 11:27:09.249237	Routerbo_f5:4d:9d	CDP/VTP/DTP/PAgP/UDLD	CDP	109	Device ID: MikroTik Port ID: bridgeLocal
84	2020-04-09 11:27:09.249237	Routerbo_f5:4d:9d	LLDP_Multicast	LLDP	121	TTL = 120 SysName = MikroTik SysDesc = MikroTik RouterOS 6.39.2 (stable) RB951U…
85	2020-04-09 11:27:10.433421	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
86	2020-04-09 11:27:10.838740	0.0.0.0	255.255.255.255	MAC-Te…	64	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Acknowled…
87	2020-04-09 11:27:10.845850	192.168.1.2	255.255.255.255	MAC-Te…	121	38:d5:47:49:ed:c7 > 64:d1:54:f5:4d:9d Direction: Client->Server Type: Data
88	2020-04-09 11:27:10.847348	0.0.0.0	255.255.255.255	MAC-Te…	64	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Acknowled…
89	2020-04-09 11:27:10.847752	192.168.1.2	255.255.255.255	MAC-Te…	125	38:d5:47:49:ed:c7 > 64:d1:54:f5:4d:9d Direction: Client->Server Type: Data
90	2020-04-09 11:27:10.848348	0.0.0.0	255.255.255.255	MAC-Te…	122	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Data
91	2020-04-09 11:27:10.848669	0.0.0.0	255.255.255.255	MAC-Te…	64	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Acknowled…
92	2020-04-09 11:27:10.848865	192.168.1.2	255.255.255.255	MAC-Te…	64	38:d5:47:49:ed:c7 > 64:d1:54:f5:4d:9d Direction: Client->Server Type: Acknowled…
93	2020-04-09 11:27:10.853674	0.0.0.0	255.255.255.255	MAC-Te…	451	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Data
94	2020-04-09 11:27:10.854186	192.168.1.2	255.255.255.255	MAC-Te…	64	38:d5:47:49:ed:c7 > 64:d1:54:f5:4d:9d Direction: Client->Server Type: Acknowled…
95	2020-04-09 11:27:12.434686	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
96	2020-04-09 11:27:14.437058	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
97	2020-04-09 11:27:16.439214	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
98	2020-04-09 11:27:18.441488	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
99	2020-04-09 11:27:20.444015	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
100	2020-04-09 11:27:20.848619	0.0.0.0	255.255.255.255	MAC-Te…	64	64:d1:54:f5:4d:9d > 38:d5:47:49:ed:c7 Direction: Server->Client Type: Acknowled…
101	2020-04-09 11:27:22.446355	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
102	2020-04-09 11:27:24.448368	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
103	2020-04-09 11:27:26.449844	Routerbo_f5:4d:9e	Spanning-tree-(for-br…	STP	60	RST. Root = 32768/0/64:d1:54:f5:4d:9d Cost = 0 Port = 0x8004
104	2020-04-09 11:27:28.238329	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.3
105	2020-04-09 11:27:28.248801	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.199? Tell 192.168.1.3
106	2020-04-09 11:27:28.259135	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.166? Tell 192.168.1.3

Gambar 6. Tampilan Data Hasil Scanning Jaringan

Analysis (Analisis)

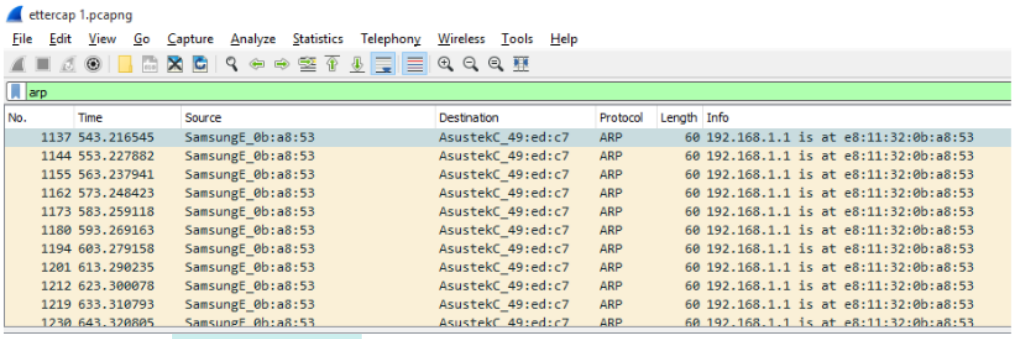
Pada tahap ini data yang berhasil dari tahap sebelumnya (examintaion) diproses kembali dengan hanya melihat pada protocol ARP untuk mencari serangan ARP *spoofing*. Lalu lintas jaringan normal terjadi ketika alamat MAC *address* yang dituju sesuai dengan alamat yang sebenarnya, dapat dilihat pada gambar 7.



No.	Time	Source	Destination	Protocol	Length	Info
31	17.912888	AsustekC_49:ed:c7	Routerbo_f5:4d:9d	ARP	42	Who has 192.168.1.1? Tell 192.168.1.2
32	17.913904	Routerbo_f5:4d:9d	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at 64:d1:54:f5:4d:9d
68	43.912633	AsustekC_49:ed:c7	SamsungE_0b:a8:53	ARP	42	Who has 192.168.1.3? Tell 192.168.1.2
69	43.913665	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.3 is at e8:11:32:0b:a8:53
71	44.162401	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	Who has 192.168.1.2? Tell 192.168.1.3
72	44.162428	AsustekC_49:ed:c7	SamsungE_0b:a8:53	ARP	42	192.168.1.2 is at 38:d5:47:49:ed:c7
104	79.869364	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.3
105	79.879836	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.199? Tell 192.168.1.3
106	79.890170	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.166? Tell 192.168.1.3
107	79.900506	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.136? Tell 192.168.1.3
108	79.911068	SamsungE_0b:a8:53	Broadcast	ARP	60	Who has 192.168.1.111? Tell 192.168.1.3

Gambar 7. Proses *Capture* Lalu Lintas Jaringan Normal

Pada gambar 7 baris nomor 31, PC 1 menghubungi *router*, terlihat pada kolom *source* (pengirim/PC1) menghubungi IP *address* 192.168.1.1 (*routerboard*). *Routerbard* memberikan balasan, pada baris no 32, bahwa IP *address* 192.168.1.1 berada pada MAC *address* 64:d1:54:f5:4d:9d. Lalu lintas jaringan tidak normal terjadi ketika alamat MAC *address* yang dituju tidak sesuai dengan alamat yang sebenarnya, atau menuju kepada alamat PC penyerang, dapat dilihat pada gambar 8.



No.	Time	Source	Destination	Protocol	Length	Info
1137	543.216545	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1144	553.227882	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1155	563.237941	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1162	573.248423	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1173	583.259118	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1180	593.269163	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1194	603.279158	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1201	613.290235	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1212	623.300078	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1219	633.310793	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53
1230	643.320805	SamsungE_0b:a8:53	AsustekC_49:ed:c7	ARP	60	192.168.1.1 is at e8:11:32:0b:a8:53

Gambar 8. Proses *Capture* Lalu Lintas Jaringan ARP *Spoofing*

Pada gambar 8 PC 2 (MAC *address* e8:11:32:0b:a8:53) memberikan *broadcast* pada PC 1 (MAC *address* 38:d5:47:49:eD:c7), bahwa *router* (IP *address* 192.168.1.1) berada pada MAC *address* PC 2 (MAC *address* e8:11:32:0b:a8:53). Hasil dari scanning jaringan menggunakan wireshark, mendapatkan informasi, berupa waktu terjadinya serangan, MAC *address* penyerang dan korban, sehingga dapat membantu investigator dalam membuat laporan kasus penyerangan ARP *spoofing* pada jaringan.

Report (Laporan)

Pada tahap ini hasil yang didapatkan dari tahapan analisis disajikan dalam bentuk laporan. Laporan yang disajikan terdiri dari informasi mengenai serangan yaitu sumber serangan dan korban beserta waktu terjadinya serangan.

SIMPULAN

Pengujian yang dilakukan dengan metode NIST dimulai dengan mengumpulkan informasi *study literature* dan membuat simulasi dengan tujuan untuk mengidentifikasi serangan ARP Spoofing. Pada tahapan simulasi dilakukan 2 serangan ARP *Spoofing* terhadap 1 perangkat laptop dan 1 perangkat *routerboard* yang terhubung didalam jaringan. Hasil dari simulasi serangan berhasil ditemukan 2 serangan beserta informasi yang berhasil diperoleh, yaitu alamat MAC *address* penyerang dan korban beserta waktu terjadinya serangan. Berdasarkan hasil pengujian yang dilakukan berhasil ditemukan semua serangan ARP *Spoofing* yang terjadi pada jaringan dengan tingkat keberhasilan 100%.

REFERENSI

Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.5665

Didi Susianto, I. Y. (2015). Mengamankan Wireless Dengan Menggunakan Two Factor, Password dan Mac Address Filtering. *Jurnal Manajemen Sistem Informasi Dan Teknologi Volume*, *05*(02), 31–36.

Fadlil, A., Riadi, I., & Aji, S. (2017). Review of detection DDOS attack detection using naive bayes classifier for network forensics. *Bulletin of Electrical Engineering and Informatics*, *6*(2), 140–148. https://doi.org/10.11591/eei.v6i2.605

Jayani, D. H. (2019). Berapa Pengguna Internet di Indonesia? *Databoks*, 1. https://databoks.katadata.co.id/datapublish/2019/09/09/berapa-pengguna-internet-di-indonesia

Kamajaya, G. E. A., Riadi, I., Prayudi, Y., & Dahlan, U. A. (2020). *Analisa Investigasi Static Forensics Serangan Man In The Arp Poisoning Based On Man In The Middle Attack In Static*. *3*(1), 6–12. https://doi.org/10.33387/jik

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2020). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410.

Mualfah, D., & Riadi, I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. *IJCSIS) International Journal of Computer Science and Information Security*, *15*(2), 326–331. https://doi.org/10.1016/j.ecss.2004.08.013

Riadi, I., Fadlil, A., & Aulia, M. I. (n.d.). *Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)*.

Riadi, I., Sunardi, S., & Rauli, M. E. (2018). Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics. *Jurnal Teknik Elektro*, *10*(1), 18–22. https://doi.org/10.15294/jte.v10i1.14070

Riadi, I., Sunardi, S., & Rauli, M. E. (2019). Live Forensics Analysis of Line App on Proprietary Operating System. *Kinetik: Game Technology, Information System,*

Computer Network, Computing, Electronics, and Control, *4*(4), 305–314. https://doi.org/10.22219/kinetik.v4i4.850

Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification of Digital Evidence on Android's Blackberry Messenger using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(5), 3–8.

Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2017). Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute of Standards and Technology (Nist). *Seminar Nasional Teknologi Informasi Dan Komunikasi - SEMANTIKOM*, 161–166.

Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). *Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)*. *4*, 219–227.

Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *7*(4), 382–390.

Syahib, M. I., Riadi, I., & Umar, R. (2020). Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST). *Jurnal Sains Komputer & Informatika (J-Sakti)*, *4*(1), 170–178.

Veny Charnita Br Ginting, Mahendra Data, D. P. K. (2019). *Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket*. *3*(5), 5049–5057.

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Performance Comparison of Forensic Software for Carving Files using NIST Method. *Jurnal Teknologi Dan Sistem Komputer*, *7*(3), 89. https://doi.org/10.14710/jtsiskom.7.3.2019.89-92

HASIL CEK_60020397_C67-Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology

ORIGINALITY REPORT

10%	8%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Jiyeon Kim, Minsun Shim, Seungah Hong, Yulim Shin, Eunjung Choi. "Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning", Applied Sciences, 2020 Publication	1%
2	Submitted to National College of Ireland Student Paper	1%
3	jurnalaspikom.org Internet Source	1%
4	pt.scribd.com Internet Source	1%
5	doku.pub Internet Source	1%
6	Submitted to Study Group Australia Student Paper	1%
7	amadakr.blogspot.com Internet Source	1%

8	journal.unnes.ac.id Internet Source	1%
9	jurnalfti.unmer.ac.id Internet Source	1%
10	123dok.com Internet Source	1%
11	jtsiskom.undip.ac.id Internet Source	1%
12	Anton Yudhana, Imam Riadi, Faizin Ridho. "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics", International Journal of Advanced Computer Science and Applications, 2018 Publication	1%
13	brilliantiririn.wordpress.com Internet Source	1%
14	zombiedoc.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		