8 (2) July 2022 156-169 ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
Register: *Jurnal Ilmiah Teknologi Sistem Informasi*

Contents lists available at www.journal.unipdu.ac.id

Register

Journal Page is available to www.journal.unipdu.ac.id/index.php/register

Research article

Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method

Agus Wijayanto [a,*], *Imam Riadi* [b], *Yudi Prayudi* [c], *Tri Sudinugraha* [d]

[a,c] *Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[b] *Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[d] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Sarawak, Malaysia*
email: [a,*]agus.wijayanto@students.uii.ac.id, [b] imam.riadi@is.uad.ac.id, [c] prayudi@uii.ac.id, [d] 21010065@siswa.unimas.my
* *Correspondence*

ARTICLE INFO

Article history:
Received 30 June 2022
Revised 18 December 2022
Accepted 28 December 2022
Available online 7 January 2023

Keywords:
Arp
Spoofing
TAARA
Tzsp
Network forensics

Please cite this article in IEEE style as:
A. Wijayanto, I. Riadi, Y. Prayudi and T. Sudinugraha, " Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 2, pp. 156-169, 2022.

ABSTRACT

This study aims to obtain attack evidence and reconstruct commonly used address resolution protocol attacks as a first step to launch a moderately malicious attack. MiTM and DoS are the initiations of ARP spoofing attacks that are used as a follow-up attack from ARP spoofing. The impact is quite severe, ranging from data theft and denial of service to crippling network infrastructure systems. In this study, data collection was conducted by launching an test attack against a real network infrastructure involving 27 computers, one router, and four switches. This study uses a Mikrotik router by building a firewall to generate log files and uses the Tazmen Sniffer Protocol, which is sent to a syslog-ng computer in a different virtual domain in a local area network. The Trigger, Acquire, Analysis, Report, Action method is used in network forensic investigations by utilising Wireshark and network miners to analyze network traffic during attacks. The results of this network forensics obtain evidence that there have been eight attacks with detailed information on when there was an attack on the media access control address and internet protocol address, both from the attacker and the victim. However, attacks carried out with the KickThemOut tool can provide further information about the attacker's details through a number of settings, in particular using the Gratuitous ARP and ICMP protocols.

1. Introduction

The integration of the use of the internet network into people's daily life is increasing. Some activities cannot be separated from the internet network, and it even becomes a basic need among a certain community. Today internet networks can support various daily needs. By utilising devices connected via the internet, the user will not need to spend extra energy and time to obtain information. All information in the world can be obtained in seconds or even faster [1]. All areas, such as education, industry, social, or banking, cannot be separated from the use of an internet network.

The Indonesian Internet Service Providers Association (APJII) is the organisation that annually reports the Internet Penetration Rate, reporting that every year the number of internet users always increases. The survey conducted by the Indonesian Internet Service Providers Association on the Penetration Rate of internet users in Indonesia shows an increase in the past five years. In 2020, there were a total of 73.7% or 196.71 million internet users out of Indonesia's 266.91 million population. Of course, the increase in the number of internet users is caused by the increasing number of users in various domains, such as in government, education, industry, and the private sectors [2].

However, with the increasing number of users of internet network-related technology, cybercrime is inevitable, which can cause harm in terms of material, trust, and others. Cybercrime is a

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

violation involving a computer that can pose a threat or impact the privacy and security of computer systems [3].

Network-related cybercrimes, including service deprivation, man-in-the-middle attacks, and spoofing, are severely dangerous to disrupt networks, bring down systems, and steal data [4], [5]. The research results in [6] reported that requests-related attack incidents are at the highest percentage of 32.7%, which is true positive mediated by encrypted files, as shown in Figure 1 as follows.

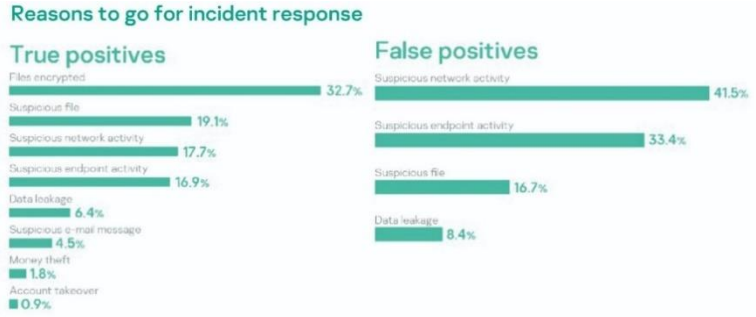


Fig. 1. Incident Response Report by Kaspersky 2021

In Figure 1, it can be seen that the number of incidents caused by suspicious network activity reaches 17.7%, which is a true positive. The highest is false positive for the incidents of suspicious network activity, accounting for 41.5%. A study by [7] shows that the number of spoofing attacks has increased by 12% from 2019 to 2021. As pointed out earlier, ARP spoofing attacks launch multiple network attacks, potentially resulting in data theft with MITM and Overburdening resources with DoS [8], [9]. The ARP protocol looks up the device's physical address before allocating a logical address to it without utilising any security measures to check ARP broadcast messages. This vulnerability would allow the execution of ARP spoofing-based cyberattacks.

A proper approach must be taken to overcome cyber attacks, so that susceptible digital evidence is kept secure [10], [11]. Network forensics is one of the techniques to overcome cyberattacks. Network forensics is a form of activity to collect, record, and analyse network traffic to find the source of the attack and other variables related to the occurring incident [12], [13]. In addition to gathering attack data and examining the characteristics of network attacks, network forensics analysis is also used to enhance network security and as a mitigation attempt [14], [15].

One of the network forensic methods is TAARA, which stands for Trigger, Acquire, Analysis, Report, and Action. This forensic method is part of the development of the Threat Assessment and Remediation Analysis Methodology, which aims to identify and assess cyber threats and select effective countermeasures to mitigate the threats [16]. Cyber attacks that make use of network technologies require response or mitigation. Some prevalent approaches, such as the forensic process model [17], [18], which has four steps, i.e., collecting phase, examination phase, analysis phase, and report phase, are not clearly linked to further activities after the reporting stage.

Another method, the National Institute of Justice (NIJ), consists of five stages: identification, collection, examination, analysis, and reporting stages [18]. This method is relatively effective in examining computer forensic cases because the process used is very different from cases involving network technology. Similarly, there are four stages in the National Institute of Standards and Technology (NIST) method[19]. Other cyberattacks will probably happen if the network forensics process ends at the finding-reporting stages. Therefore, a precise network forensic investigation stage is required to overcome the ARP spoofing cyberattack, which has an impact on other cyberattacks. The network forensic investigation is carried out to direct investigators in gathering evidence and taking preventative measures against advanced cyberattacks.

In this study, considering that the impact of a spoofing attack is the basis for starting the next attack, the TAARA method was used because it requires less scope and time. Therefore, an investigation was conducted to obtain information regarding the evidence of the assault, the identity of the assailant, and the victim. This forensic ARP spoofing is also different in terms of the angle of the investigation, that is, by scanning the Mikrotik router, which produces the Tazmen Sniffer Protocol (TZSP) by applying the TAARA method.

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

2. Materials and Methods

ARP spoofing serves as an initial attack, paving the way for other cyberattack techniques. ARP spoofing attacks can be carried out using various tools, which determine the identification of cyberattacks. A previous study by [20] discussed the prevention of vulnerabilities in the ARP protocol using multiplicative enhancement and additive reduction algorithms in detecting spoofing attacks involving an AI engine which was used to look for more parameters in the inspection process. The conceptual framework was to use an AI engine to study traffic by using an algorithm to identify suspicious traffic indications by verifying the Mac Address. Meanwhile, the semi-static technique [21] applied to defend against spoofing attacks has the disadvantage of not being able to protect other hosts.

The application of a software-defined network (SDN) that is considered the replacement of a conventional network that allows global configuration using a controller requires a lot more in-depth research on attacks that can possibly occur [22]. Many studies have detected ARP spoofing attacks, but some of the tests have a fundamental problem – not being able to confirm that the device has performed ARP instructions [23]. Recently, a survey [24] related to techniques for detecting and mitigating ARP spoofing attacks was also conducted. However, it did not provide a specific assessment or a recommendation on the best approach to prevent spoofing attacks.

The growth of cybercrime is currently being aided by freely available tools on the internet, and one type of attack can have many data characteristics. The use of network forensic science is required to combat various cybercrimes, including ARP spoofing attacks. Collecting evidence is an essential part of efforts to prove ARP spoofing attacks in the forensic network science approach. Data collection on the network can use stored logs or traffic capture. A number of previous studies captured network traffic using the Tazmen Sniffer Protocol [25]–[27]. The captured network traffic data is encapsulated in the TaZmen Sniffer Protocol (TZSP), which is then de-encapsulated and extracted. Transport layer information for each packet was acquired by listening to TZSP UDP port 37008.

The TAARA method was used in this study as a guide for carrying out the research, and a comprehensive discussion is presented in section 4. As seen in Figure 2, the TAARA approach consists of various stages.

Fig.2. The TAARA Method

The following is a brief description of how the TAARA method steps are interconnected in Fig.2.

1. Trigger is an activity that follows an assault and directs the investigator to start an investigation.
2. Acquire is the act of acquiring all available information and proof in order to surmise the origin of an attack incident. In the previous level, a trigger for suspicious behaviour led to the action of acquiring.
3. Analysis is the process of gathering evidence and information that is already available, correlating them to raise concerns about the attacks taking place.
4. Reporting is the process of writing a report based on the conclusions of the previous analysis, recording all activities involved.
5. Action is the stage where recommended suggestions are taken in response to the recommendations in the previous stage.

The framework of this research consists of eight stages, in which the TAARA method is added, which ends with validation. The stages of the current research are shown in Figure 3 as follows.

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

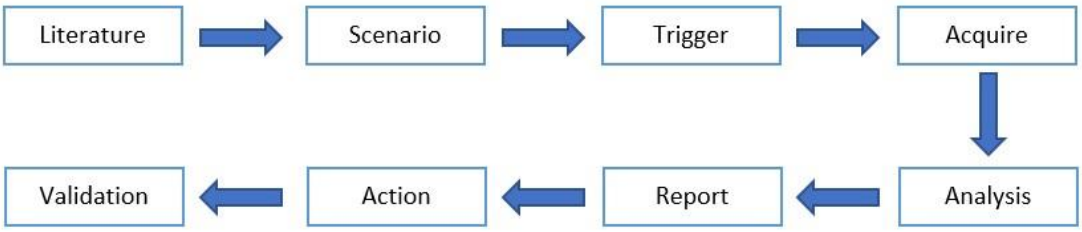


Fig.3. Research Process Flowchart

In Figure 3, it can be seen that the first step is a literature review to gather information related to the current research by referring to previous related literature sources. The next stage is to determine the attack scenario, which is implemented using equipment and materials in the laboratory. Subsequently, the stages in the TAARA method are implemented for the investigation process, from Trigger to Action. The last stage is validation, in which a test of the results obtained during the network forensics process is conducted.

2.1. Requirement Resources

The attack scenario is designed by preparing hardware and software equipment for the attack testing. Table 1 shows the complete set of requirements.

Table 1. Hardware and Software

No	Hardware and Software	Desciption
1	Asus VivoBook Max X441UV laptop with an Intel® Core™ i3-6006U processor and 12 GB RAM	attacker computer
2	Asus laptop with Intel® Core™ I7-4770 processors and 16 GB RAM	Investigator's computer
3	A computer laboratoy with 27 computers	Verified client computer
4	Mikrotik CCR1009-7G-1C-1S+ router	Network Tools
5	US-48 PoE 500w Unifi	
6	TP-Link Switch	
7	Wireshark	Tool for analysing network traffic
8	Network Miner	
9	Arpspoof	Tool for performing ARP spoofing attacks
10	KickThemOut	
11	Ettercap	
12	Bettercap	

2.2. Network Design

This network uses the infrastructure implemented at the Mulia University Laboratory. There are several network segments, but the testing was focused on the VLAN 15 segment for the attacked domain and VLAN 99 as a separate domain for Syslog. The topology details are shown in Figure 4 below.

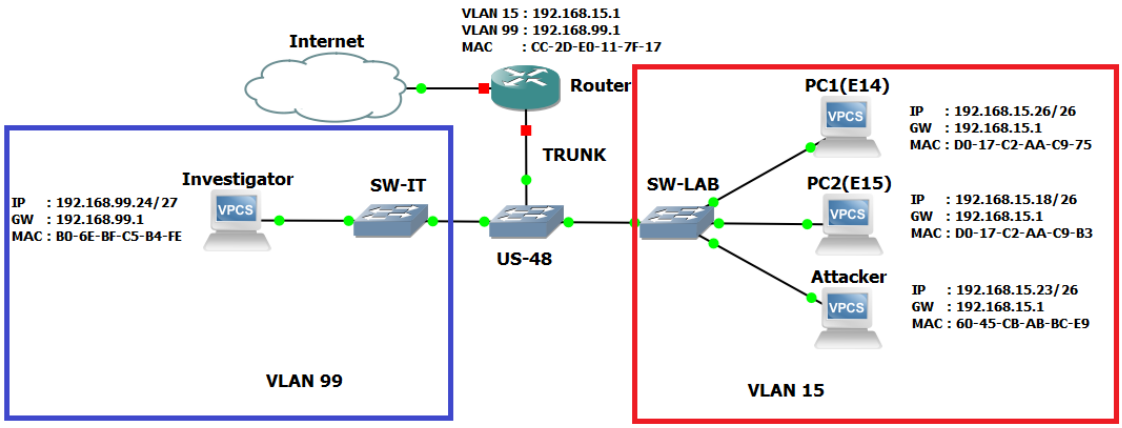


Fig.4. Network Topology

http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Figure 4 shows the launch of an ARP spoofing attack on segment VLAN 15 in the red box. There are 27 active hosts in the VLAN 15 portion of the computer laboratory. Regarding the target and the gateway address, there are two hosts in this part. Along with identity IP addresses, two active hosts have the Mac addresses 192.168.15.18 (D0-17-C2-AA-C9-95) and 192.168.15.26. (D0-17-C2-AA-C9-B3). A sniff is a network traffic sniffing tool used by the router equipment. Because the routers have a directly connected communication to their segments locally, this scanning approach can represent multiple topologies as long as there is a router. The Tazmen Sniffer Protocol is used to deliver real-time network traffic information to the investigators' computer. Configuration details are shown in Table 2 as follows.

Table 2. The Network Configuration

Device	VLAN	IP Address	Netmask	Gateway
Router	15	192.168.15.1	255.255.255.192	-
	99	192.168.99.1	255.255.255.224	-
Attacker	15	192.168.15.23	255.255.255.192	192.168.15.1
27 Active Hosts	15	192.168.15.2 – 192.168.15.61	255.255.255.192	192.168.15.1
Victim 1	15	192.168.15.18	255.255.255.192	192.168.15.1
Victim 2	15	192.168.15.26	255.255.255.192	192.168.15.1
Investigators	99	192.168.99.24	255.255.255.224	192.168.99.1

Table 2 shows the logical address configurations implemented in the laboratory network. The network infrastructure in it uses a router with firewall logging rules. Rules are built into the firewall to collect log data, as shown in Figure 5.

```
[aguswijayanto.id@Universitas Mulia] > /ip firewall filter
[aguswijayanto.id@Universitas Mulia] /ip firewall filter> add action=log chain=input in-interface=V15-Lab_Net log-prefix=INPUT
```

Fig.5. Firewall Rules

According to the rules set up on the router, the firewall logging rules in Figure 5 will collect network traffic on VLAN 15 domain. While the log_prefix serves as a log identity marker, the input chain created aims to capture all network traffic that enters the router port from VLAN 15 interface, which is directly connected to the local router port. The firewall rule's action is log, which means that it will be taken out as a log that can be put into the logging rule. The created firewall rules can then be added to the logging system. By default, system logging also displays rules such as DHCP logs, system logs, and warning logs. This log is transmitted remotely to the host computer, in this case, the investigators' computer.

2.3. Attack Simulation

The attack simulation was created using the network topology design shown in Figure 4. The attack was tested eight times with detailed explanations as follows.

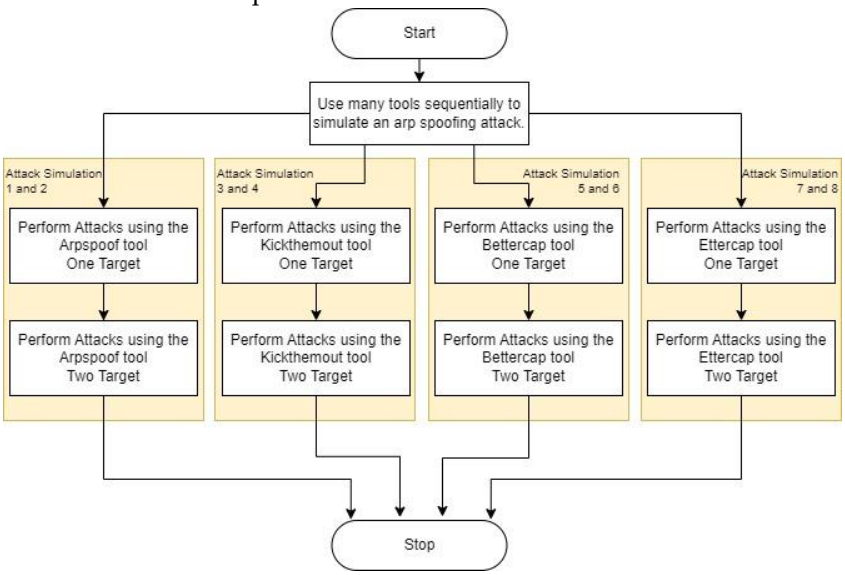


Fig. 6. Arpspoofing Attack Simulation Flow

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Figure 6 depicts the flow of the attacks in sequence. The first attack simulation begins with one target using the ARPSpoof tool. The second simulation still employs the ARPspoof tool to target two hosts simultaneously. The subsequent attack simulation employs Bettercap attack tool, making the total attack simulations eight times, including the ARP spoofing attack tests.

3. Results and Discussion

3.1. Trigger

The initial phase of the investigation is known as Trigger. A communication failure with the target host as a result of harm to the ARP table is the initial trigger for the investigation in an ARP spoofing attack. Figure 7 illustrates one example of a host's ARP table being damaged.

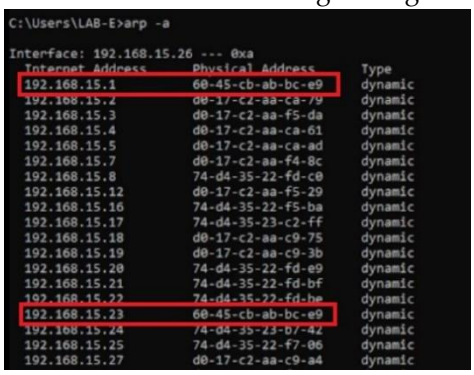


Fig. 7. Example of a host's ARP table being damaged

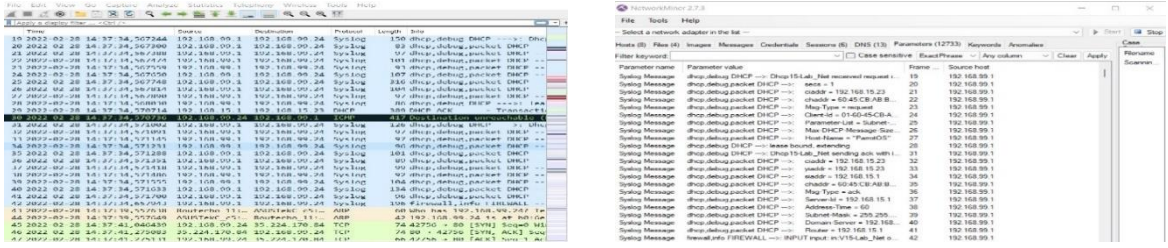
The damage to the ARP table is depicted in Figure 7 as a result of an attack using ARP spoofing. Two IP addresses are assigned to a single Mac address. This example of ARP table damage is representative of seven previous simulations of ARP spoofing assaults as the impact is the same, i.e., the damage of the ARP table.

3.2. Acquire

Based on the information obtained from the trigger stage that the ARP table on each target host has been damaged, the next step is to collect data. Network traffic data was obtained from the scanning, as described in section 3.2 above. Table 3 below shows the data collected from the investigators' computer in the form of eight Packet Capture Files (PCAP). Table 3 shows that eight files were collected, each with an MD5 Hash value, and information about the number of packets was also gathered. The most critical aspect of collecting digital evidence is ensuring data integrity. Changes to digital evidence will impact the evidence's validity or invalidity. As a result, an initial examination is required to obtain a value to ensure data integrity when gathering digital evidence. To ensure data integrity, network mining tools are used to determine the value of the MD5 Hash.

3.3. Analysis

Since ARP is stateless, an attacker can easily manipulate it to perform a spoofing attack. Because the attacker's arp-reply was being verified, the ARP table can be compromised by packets, including the victim's Mac address and IP address. Catch records from the preceding phase were also analysed, along with other results indicators. At this stage, multiple protocols emerged from the scanned data; among them is the Syslog, as seen in Figure 8 below.



(a) (b)

Figure 8. The Display of Wireshark and Network Miner Traffic

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Table 3. Data Collection Details

File	MD5 Hash	Screen Recording	Packet
PCAP-1	c31552fe97193a67fe6eff941b6d43ce	Metadata: Filename: Scanning Arpspoof - Pengujian 1.pcap; Start: 28/02/2022 06:37:09; End: 28/02/2022 06:46:23; Frames: 149975; MD5: c31552fe97193a67fe6eff941b6d43ce	149975 Packet
PCAP-2	17b17d6044210093b0fcacd86fb54828	Metadata: Filename: Scanning Arpspoof - Pengujian 2.pcap; Start: 28/02/2022 07:30:14; End: 28/02/2022 07:35:39; Frames: 68639; MD5: 17b17d6044210093b0fcacd86fb54828	68639 Packet
PCAP-3	1ddde26c242fc5fe0d006dac4cbffc70	Metadata: Filename: Scanning-Kick ThemOut-1.pcap; Start: 28/02/2022 02:53:01; End: 28/02/2022 03:02:43; Frames: 1665131; MD5: 1ddde26c242fc5fe0d006dac4cbffc70	1665131 Packet
PCAP-4	13977450cf96658368b4424dfe14b4ec	Metadata: Filename: Scanning Kick ThemOut - Pengujian 2.pcap; Start: 28/02/2022 05:44:36; End: 28/02/2022 05:57:33; Frames: 177055; MD5: 13977450cf96658368b4424dfe14b4ec	177055 Packet
PCAP-5	e7ec098464532702e689211c956e0751	Metadata: Filename: Scanning Ettercap - Pengujian 1.pcap; Start: 03/03/2022 06:23:48; End: 03/03/2022 06:31:53; Frames: 149892; MD5: e7ec098464532702e689211c956e0751	149892 Packet
PCAP-6	179431d6709d857d35948ff03c2431b1	Metadata: Filename: Scanning Ettercap - Pengujian 2.pcap; Start: 03/03/2022 06:49:42; End: 03/03/2022 06:57:49; Frames: 109337; MD5: 179431d6709d857d35948ff03c2431b1	109337 Packet
PCAP-7	bca7d692ab7d2a24975405674a68d753	Metadata: Filename: Scanning Bettercap - Pengujian 1.pcap; Start: 02/03/2022 03:36:02; End: 02/03/2022 03:47:56; Frames: 578487; MD5: bca7d692ab7d2a24975405674a68d753	578487 Packet
PCAP-8	93dc96d6514b9ff3fecec974d4eb11e2	Metadata: Filename: Scanning Bettercap - Pengujian 2.pcap; Start: 03/03/2022 02:49:43; End: 03/03/2022 02:59:43; Frames: 136143; MD5: 93dc96d6514b9ff3fecec974d4eb11e2	136143 Packet

The findings of the unfiltered network activity using Wireshark are displayed in Figure 8-a, while the information obtained using the Network Miner program is displayed in Figure 8-b. Subsequently, the ARP protocol is the primary topic of discussion in the analysis. Under typical conditions, an arp-request will be broadcast across the entire local network. Then, an arp-reply will be given in response if the host IP can successfully locate the destination IP, as described in Figure 9.

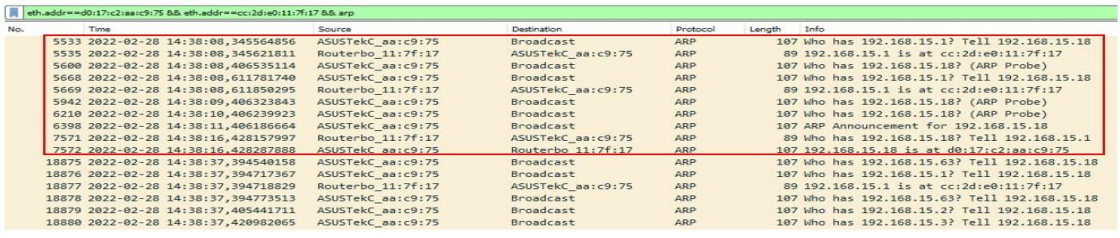


Fig. 9. ARP Protocol Normal Circumstances

As seen in Figure 8, Victim PC 1 with Address D0-17-C2-AA-C9-75 broadcasts frames 5533 of its arp-request message, asking for ownership of IP address 192.168.15.1. In packet 5535, the router identified by MAC address CC-2D-E0-11-7F-17 responds to an arp-request by providing the information that its IP address is 192.168.15.1. Frames 5600, 5942, and 6210 all show Addresses D0-17-

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

C2-AA-C9-75 (Victim 1), broadcasting ARP Probe information seeking IP address 192.168.15.18. The existence of the Address 192.168.15.18 is verified through an ARP query.

Then, the respondent will emphasize that the IP address corresponding to MAC address D0-17-C2-AA-C9-75 is 192.168.15.18, as described in frame 6398. The routers and Target PC 1 have established the IP address–MAC address mapping in frames 7571 and 7572. Table 4 displays in the first place where time is utilised as a mapping key for arp-request and arp-reply messages.

Table 4. ARP Message Mapping

Time	Source	Destination	Description
28/02/2022 14:38:08	d0:17:c2:aa:c9:75	00:00:00:00:00:00	Arp-request
28/02/2022 14:38:08	cc:2d:e0:11:7f:17	d0:17:c2:aa:c9:75	Arp-reply
28/02/2022 14:38:16	cc:2d:e0:11:7f:17	d0:17:c2:aa:c9:75	Arp-request
28/02/2022 14:38:16	d0:17:c2:aa:c9:75	cc:2d:e0:11:7f:17	Arp-reply

In table 4, the arp-reply message carries information in the form of IP ownership, in which IP information has been recorded to the MAC address of the device. When an ARP spoofing attack occurs, the attacker will try to poison the arp table by giving a message in the form of an arp-reply. The victim's IP address is shown in Figure 10 below.

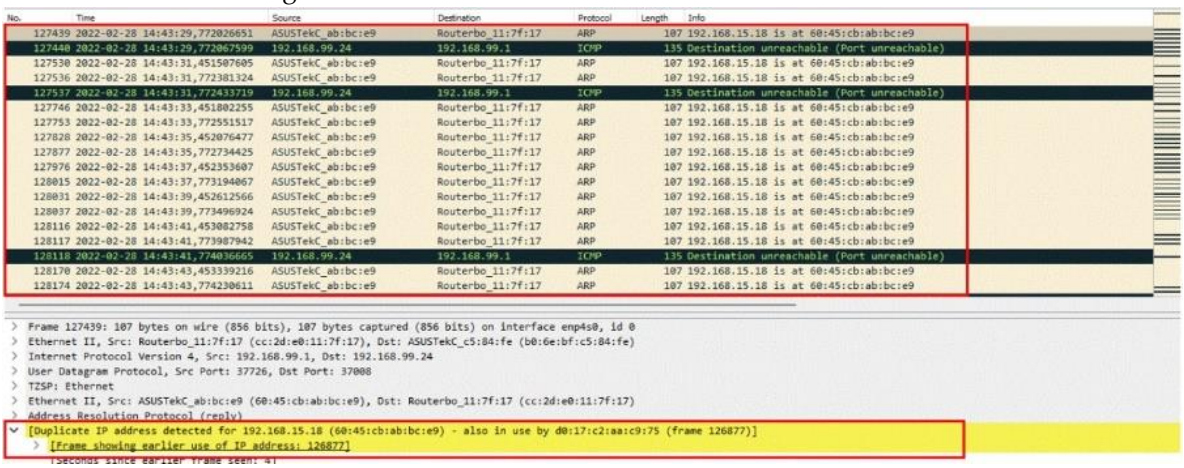
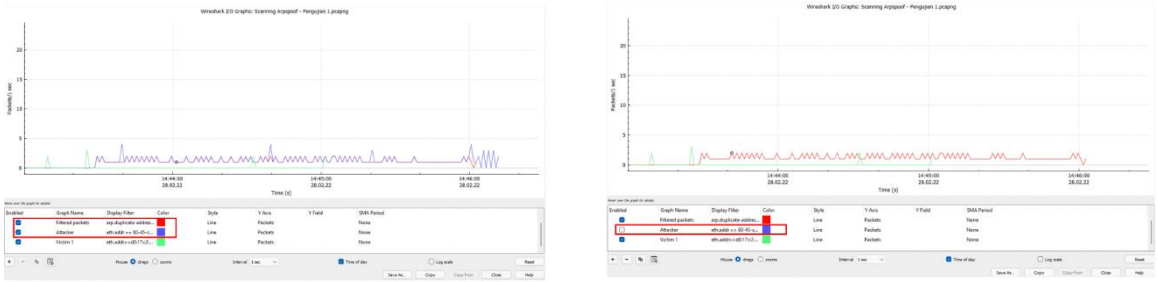


Fig. 10. The Display of Network Traffic During ARP spoofing Attempts

In figure 8, the attacker with MAC Address 60-45-CB-AB-BC-E9 sends an arp-reply message, informing that IP 192.168.15.18 is the attacker's IP. It is different from the first finding in Figure 10, in which IP Address 192.168.15.18 has MAC Address D0-17-C2-AA-C9-75. A filter is then performed to display a statistical I/O graph, as shown in Figure 11 below.



(a) (b)

Fig. 11. I/O Graphs

In Figure 9, I/O Graph can display a graph based on a customised filter. There are three filter rules to show I/O graph comparisons of ARP duplicate detection, the attacker's MAC, and the victim's MAC. The red colour indicates the filter result of the similarly detected ARP; the blue colour indicates the filter of the attacker's MAC address; while the green colour indicates the filter of the victim MAC address.

The red and blue parts of A relatively have the same I/O Graph. They are more explicit when the blue filter is unchecked, as seen in area B. Section B shows the red color, which has the same Graph I/O as the blue one shown in section A. This fact indicates that network traffic with the ARP filter duplicates the network address that found the traffic owned by the attacker. However, it is found that the victim's network traffic is marked in green, which indicates that there is no finding through the arp duplicate

http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

filter. It is essential to note that the final analysis on attack testing using KickThemOut is slightly different from the findings obtained, as shown in Figure 12.

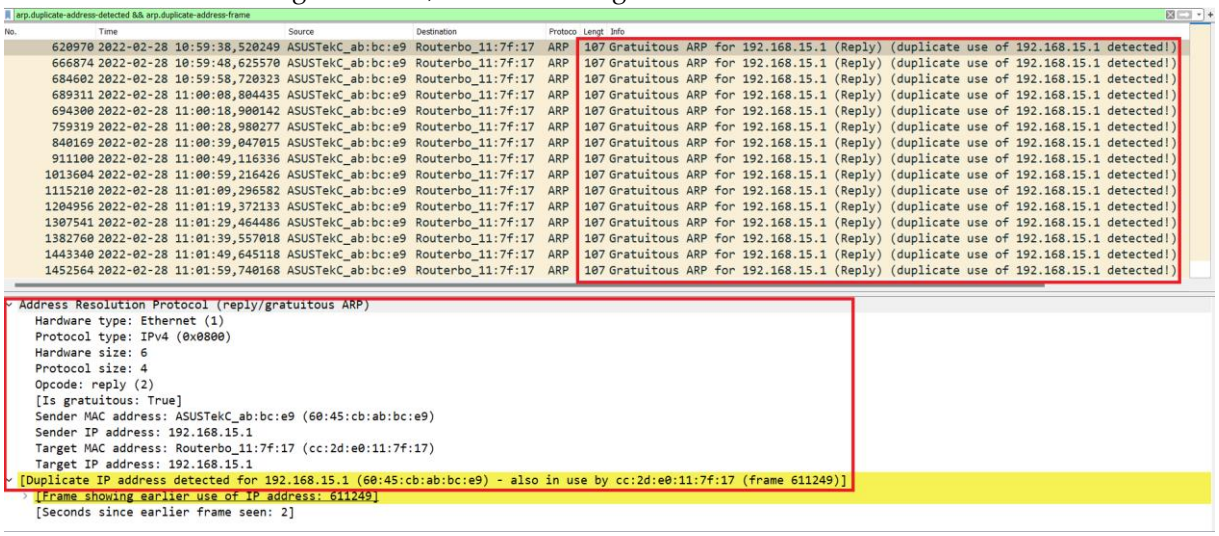


Fig. 12. Display of Network Traffic During a spoofing Attack Utilising The KickThemOut Tool

In Figure 10, it can be seen that the attack scheme is carried out the same as before, that is by sending an arp-reply packet. The information obtained using the duplicate ARP filter is an arp-reply in the form of a Gratuitous ARP to the router. Attacks done using KickThemOut do not precisely specify which victims were attacked, but they can still be identified through thorough identification involving other protocols, as described in Figure 13.

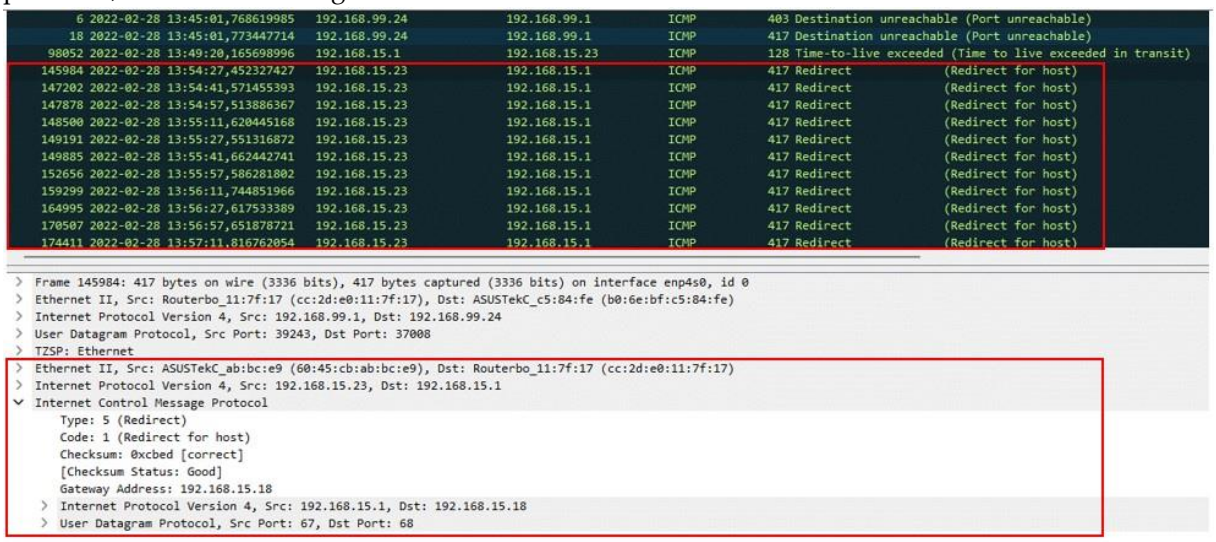


Fig. 13. Redirect Packet

Figure 13 above shows the existence of a packet redirect or packet transfer as a result of the attack carried out. First, it indicates that a spoofing attack has been carried out, causing a diversion of network communications. Second, the search focus is not only on the ARP protocol, but is also expanded to include the ICMP protocol to obtain attack evidence. Third, this spoofing attack shows that the communication between the router 192.168.15.1 to the victim's computer 192.168.15.18 results in packet diversion from the attacker's computer 192.168.15.23.

3.4. Report

At this stage, the report provides a summary of all the actions carried out in the previous steps. The report stage provides information about the incident, including the identity of the attacker and the victim. At this stage, the report is prepared meticulously in detail, attempting to describe the information in a table, including the details of the attack's timing.

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Table 5. The Report Evidence of the Attacks

No	Attacker	Victims	Times of Attacks	Frame Number	No	Attacker	Victim	Times of Attacks	Frame Number
1	192.168.15.23	192.168.15.18	28/02/2022 14:43:30	127439	5	192.168.15.23	192.168.15.18	03/03/2022 14:28:12	78204
2	192.168.15.23	192.168.15.18	28/02/2022 15:33:23	45034	6	192.168.15.23	192.168.15.18	03/03/2022 14:54:34	58076
		192.168.15.26	28/02/2022 15:33:25	45301			192.168.15.26	03/03/2022 14:54:34	58080
3	192.168.15.23	192.168.15.18	02/03/2022 11:45:53	537266	7	192.168.15.23	192.168.15.18	28/02/2022 11:01:40	1382667
4	192.168.15.23	192.168.15.18	03/03/2022 10:54:15	55489	8	192.168.15.23	192.168.15.18	28/02/2022 13:54:27	145984
		192.168.15.26	03/03/2022 10:54:15	55490			192.168.15.26	28/02/2022 13:54:42	147202

The ARP spoofing attack details, including time, attacker, and targets, are summarised in Table 6. A summary of the evidence data can be seen in Figure 14.

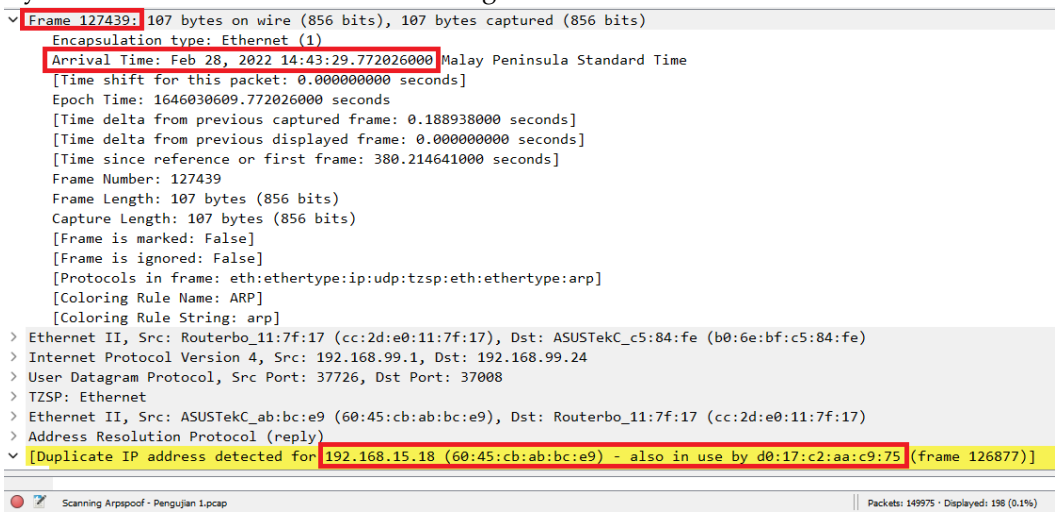


Fig. 14. PCAP-1 file contains ARP spoofing attack evidence.

Figure 14 outlines the information presented in table 5, number 1 of this study. Evidence-related information can be discovered in Frame 127439, along with time-related information. This frame shows that there was a duplication of IP addresses. The attacker's MAC Address, 60:45:cb:ab:bc:e9, uses the IP address 192.168.15.18, which has already been used by MAC Address d0:17:c2:aa:c7:75, per instructions from frame 126877. In this paper, we have demonstrated the detailed attack information in Table 5.

3.5. Action

Suggestions for actions to be carried out are included in the report produced. The actions to halt ARP spoofing attacks and prevent any other sophisticated attacks are in accordance with the findings of the ARP spoofing investigation using the TAARA approach. Isolating the attacker's 60:45:cb:ab:bc:e9 MAC address is a step to stop ongoing attacks because, according to the report's findings, information on the attacker's identification address was discovered.

3.6. Validation

Verifying the authenticity, accuracy, and credibility of the findings of the forensic analysis is an essential step, so that they can be used as acceptable evidence in court. In addition, it is necessary to confirm that the findings can account for data integrity. Findings from forensic investigations can be used as digital evidence if, as [28] claimed, they can be verified independently.

The attack tests using all four tools are validated on a repeatable basis by utilising the Wireshark analysis tool. The PCAP file obtained was then inspected by both the network miner and Wireshark. Network miner data shows no signs of an impending attack.

 http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Table 6. Repeatability validation results

Evidence	Wireshark							
	ARP Spoof		KickThemOut		Ettercap		Bettercap	
	PCAP-1	PCAP-2	PCAP-3	PCAP-4	PCAP-5	PCAP-6	PCAP-7	PCAP-8
Frames	149975	68639	1665131	177055	149892	109337	578487	136143
Attacker's IP	obtained	obtained	obtained	obtained	obtained	obtained	obtained	obtained
Attacker's MAC	obtained	obtained	obtained	obtained	obtained	obtained	obtained	obtained
Victims' MAC	obtained	obtained	obtained	obtained	obtained	obtained	obtained	obtained
Victims' IPs	obtained	obtained	obtained	obtained	obtained	obtained	obtained	Obtained
Timestamp	obtained	obtained	obtained	obtained	obtained	obtained	obtained	Obtained
Syslog	obtained	obtained	obtained	obtained	obtained	obtained	obtained	Obtained
Evidence	**Network Miner**							
	ARP Spoof		KickThemOut		Ettercap		Bettercap	
	PCAP-1	PCAP-2	PCAP-3	PCAP-4	PCAP-5	PCAP-6	PCAP-7	PCAP-8
Frames	149975	68639	1665131	177055	149892	109337	578487	136143
Attacker's IP	not found	not found	not found	not found	not found	not found	not found	not found
Attacker's MAC	not found	not found	not found	not found	not found	not found	not found	not found
Victims' MAC	not found	not found	not found	not found	not found	not found	not found	not found
Victims' IPs	not found	not found	not found	not found	not found	not found	not found	not found
Timestamp	not found	not found	not found	not found	not found	not found	not found	not found
Syslog	obtained	obtained	obtained	obtained	obtained	obtained	obtained	Obtained

Table 6 illustrates the results of repeated tests of Wireshark's performance in detecting ARP spoofing attacks against the TZSP protocol's implementation.

The length of time spent to validate an experiment distinguishes a repeatability test from a reproducibility test. A reproducibility test is conducted using the same materials and methods across an extended time frame. Meanwhile, the repeatability of the tools employed has been verified in the preceding phase.

Table 7. The Results of reproducibility validation

Evidence	Wireshark							
	ARP Spoof		KickThemOut		Ettercap		Bettercap	
	PCAP-1	PCAP-2	PCAP-3	PCAP-4	PCAP-5	PCAP-6	PCAP-7	PCAP-8
Frames	149975	68639	1665131	177055	149892	109337	578487	136143
IP Attacker	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
Mac Attacker	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
MAC Victim	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
IP Victim	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
Timestamp	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
Syslog	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	obtained
Evidence	**Network Miner**							
	ARP Spoof		KickThemOut		Ettercap		Bettercap	
	PCAP-1	PCAP-2	PCAP-3	PCAP-4	PCAP-5	PCAP-6	PCAP-7	PCAP-8
Frames	149975	68639	1665131	177055	149892	109337	578487	136143
IP Attacker	not found	not found	not found	not found	not found	not found	not found	not found
Mac Attacker	not found	not found	not found	not found	not found	not found	not found	not found
MAC Victim	not found	not found	not found	not found	not found	not found	not found	not found
IP Victim	not found	not found	not found	not found	not found	not found	not found	not found
Timestamp	not found	not found	not found	not found	not found	not found	not found	not found
Syslog	obtained	Obtained	obtained	obtained	obtained	obtained	obtained	Obtained

http://doi.org/10.26594/register.v8i2.2953

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Table 7 presents the repeatability validation with the same findings, indicating that evidence of an attack can be reported using the Wireshark forensic tool. However, network miners cannot obtain the entire TZSP protocol details.

4. Conclusion

Investigating network forensics by applying the TAARA method can help investigators to obtain evidence of systematic ARP spoofing attacks. A series of test attacks on real network infrastructure was carried out using spoofing attacks with four command-based and GUI-based tools. However, different attack characteristics were obtained when using the KickThemOut tool. The search for evidence requires more effort by involving the ICMP protocol to acquire information. In addition, the scan results performed using a router that sends all packets, including the TZSP protocol, can be analysed thoroughly using the Wireshark tool, but not the network miner tool. The attack evidence was apparent as we obtained the attacker's MAC and IP addresses as well as the time and date of the attacks, which were all easily deciphered using Wireshark forensic tools. The network forensic investigations revealed that the attack was launched eight times, and this was noted as evidence in the investigation report.

Author Contributions

A. Wijayanto: Writing – original draft, Experiment. I. Riadi: Methodology and review. Y. Prayudi: Review and writing. T. Sudinugraha: Validating.

Declaration of Competing Interest

We declare that we have no conflict of interest.

References

[1] M. Farooq and Q. A. Qureshi, "Privacy of Internet Users in the Era of Transformative Marketing," *Journal of Management Practices, Humanities and Social Sciences*, vol. 4, no. 2, pp. 25–28, 2020.

[2] A. Wicaksono and H. Herdiansyah, "The internet of things (iot) for flood disaster early warning in DKI Jakarta: prospect and community preparedness," *IOP Conf Ser Earth Environ Sci*, vol. 683, no. 1, p. 012103, Mar. 2021, doi: 10.1088/1755-1315/683/1/012103.

[3] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

[4] O. A. Hussein, N. A. Manap, M. Rizal, A. Rahman, B. Muntadher, and A. Wahhab, "Cyber Blackmail on Social Media and its Authenticity through Criminal Evidence Cyber Blackmail on Social Media and its Authenticity through Criminal Evidence," *NeuroQuantology*, vol. 20, no. 6, pp. 121–132, 2022, doi: 10.14704/nq.2022.20.6.NQ22014.

[5] E. Staddon, V. Loscri, and N. Mitton, "Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey," *Applied Sciences*, vol. 11, no. 16, p. 7228, Aug. 2021, doi: 10.3390/app11167228.

[6] Kaspersky, "Incident Response Analyst Report 2021." 2021. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/13085018/Incident-Response-Analyst-Report-eng-2021.pdf

[7] A. Berg and S. Selen, "bitkom 2021," no. August, p. 19, 2021.

[8] J. Muungano, "How Organisations Become Exposed to Certain Cyber-Attacks or Breaches and Ways to Mitigate", doi: 10.14704/nq.2022.20.6.NQ22422.

[9] S. Rao Allanki, N. Venu, D. Kumar, and As. Rao, "Botnet Attacks Detection In Internet Of Things Using Machine Learning Botnet Attacks Detection In Internet Of Things

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

Using Machine Learning" NeuroQuantology 2022; 20(4): 743-754, vol. 20, 2022, doi: 10.14704/NQ.2022.20.4.NQ22298.

[10] I. Riadi, M. Sumagita, A. Dahlan, I. Jl Soepomo Sh, K. Yogyakarta, and D. Istimewa Yogyakarta, "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," 2018. [Online]. Available: https://www.researchgate.net/publication/327392778

[11] I. Riadi, "Examination of Digital Evidence on Android-based LINE Messenger," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, pp. 336–343, 2018, doi: 10.17781/P002472.

[12] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, Sep. 2020, doi: 10.1016/j.future.2020.03.042.

[13] Subektiningsih, Y. Prayudi, and I. Riadi, "Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, p. 294+, 2018, [Online]. Available: https://link.gale.com/apps/doc/A570819767/AONE?u=anon~5850c42d&sid=googleScholar&xid=9f19e9d5

[14] A. v Kachavimath, S. V. Nazare, and S. S. Akki, "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Mar. 2020, pp. 711–717. doi: 10.1109/ICIMIA48430.2020.9074929.

[15] A. R. Caesarano and I. Riadi, "Network Forensics for Detecting SQL Injection Attacks Using NIST Method," 2018. [Online]. Available: https://www.researchgate.net/publication/328135106

[16] R. Umar, I. Riadi, and R. S. Kusuma, "Network Forensics Against Ryuk Ransomware Using Trigger , Acquire , Analysis , Report , and Action (TAARA) Methods," vol. 4, pp. 197–204, 2021.

[17] I. Riadi, J. E. Istiyanto, A. Ashari, and Subanar, "Log Analysis Techniques using Clustering in Network Forensics," vol. 10, no. 7, 2013, [Online]. Available: http://arxiv.org/abs/1307.0072

[18] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int J Comput Appl*, vol. 177, no. 27, pp. 35–42, Dec. 2019, doi: 10.5120/ijca2019919749.

[19] B. Suhardjono, A. Syah Putra, N. Aisyah, and V. Valentino, "Analysis Of Nist Methods On Facebook Messenger For Forensic Evidence," no. 8, 2022.

[20] M. Anathi and K. Vijayakumar, "An intelligent approach for dynamic network traffic restriction using MAC address verification," *Comput Commun*, vol. 154, pp. 559–564, 2020, doi: 10.1016/j.comcom.2020.02.021.

[21] M. Data, "The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table," *3rd International Conference on Sustainable Information Engineering and Technology, SIET 2018 - Proceedings*, pp. 206–210, 2018, doi: 10.1109/SIET.2018.8693155.

[22] T. Girdler and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (2) July 2022 156-169

and Blacklisted MAC Addresses," *Computers and Electrical Engineering*, vol. 90, no. July 2020, p. 106990, 2021, doi: 10.1016/j.compeleceng.2021.106990.

[23] Z. Miao, G. Liu, H. Wang, and Y. Wang, "Dynamic Trust Model of ARP Real-Time Intrusion Detection Based on Extended Subjective Logic," *Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2020*, no. 1705, pp. 615–618, 2020, doi: 10.1109/ICPICS50287.2020.9201994.

[24] V. Rohatgi and S. Goyal, "A detailed survey for detection and mitigation techniques against ARP spoofing," *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, pp. 352–356, 2020, doi: 10.1109/I-SMAC49090.2020.9243604.

[25] G. Vira Yudha and R. Wisnu Wardhani, "Design of a Snort-based IDS on the Raspberry Pi 3 Model B+ Applying TaZmen Sniffer Protocol and Log Alert Integrity Assurance with SHA-3," in *2021 9th International Conference on Information and Communication Technology (ICoICT)*, Aug. 2021, pp. 556–561. doi: 10.1109/ICoICT52021.2021.9527511.

[26] G. B. Gavilanes, "Persons counter through Wi-Fi's passive sniffing for IoT," in *2018 IEEE Third Ecuador Technical Chapters Meeting (ETCM)*, Oct. 2018, pp. 1–6. doi: 10.1109/ETCM.2018.8580283.

[27] P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," *Computers & Electrical Engineering*, vol. 73, pp. 84–96, Jan. 2019, doi: 10.1016/j.compeleceng.2018.11.004.

[28] E. OliveiraJr, A. F. Zorzo, and C. V. Neu, "Towards a conceptual model for promoting digital forensics experiments," *Forensic Science International: Digital Investigation*, vol. 35, p. 301014, Dec. 2020, doi: 10.1016/j.fsidi.2020.301014.