Research Article

Implementation of Webservice Security: A Case Study on HTTPS Usage and ARP Spoofing Attack Threats

[1*]Novi Aryani Fitri, [2]Okta Maulana

[1,2] Politeknik Negeri Pontianak, Kec. Pontianak Tenggara, Pontianak City, West Kalimantan 78124, Indonesia

* Corresponding Author: noviaryanif@polnep.ac.id

Abstract: This study explores network security within a simulated environment built using VirtualBox, focusing on comparing the HTTP and HTTPS protocols in protecting data from eavesdropping. The research follows the PPDIOO model (Prepare, Plan, Design, Implement, Operate, and Optimize), including system requirements mapping and the setup of a virtual network environment that supports VLAN and data security. Two main scenarios were tested: an authorized user securely accesses a server using HTTPS, and another where an attacker attempts to intercept communication between the client and server using HTTP. The results indicate that HTTPS effectively protects data from eavesdropping attempts by attackers, while HTTP leaves security vulnerabilities that can be exploited to steal sensitive information. This study underscores the importance of using secure protocols like HTTPS in VLAN-based networks to protect data from eavesdropping and other threats. Additionally, the research paves the way for developing further security measures in network management, such as firewalls, intrusion detection systems (IDS), and more advanced encryption.

Keywords: VLAN; Webservice; ARP Spoofing; Wireshark; Network Security

Citation: N.A.Fitri & Maulana, O. "Implementation of Webservice Security: A Case Study on HTTPS Usage and ARP Spoofing Attack Threats", *Iota*, **2024**, ISSN 2774-4353, Vol.04, 03. https://doi.org/10.31763/iota.v4i3.805

Academic Editor : Adi, P.D.P

Received : July, 12 2024

Accepted : July, 15 2024

Published : August, 15 2024

Publisher's Note: ASCEE stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Technology development within networks has experienced significant growth in recent years, driven by the increasing number of devices, applications, and services requiring connectivity. Factors such as online learning, collaborative research, and the Internet of Things have further increased the complexity and scale of networks. In computer networks that often serve thousands of users and handle sensitive data, they become an attractive target for cyber attackers. As a result, ensuring the security of campus networks has become a top priority for network administrators and security professionals.

Virtual Local Area Networks (VLANs) have emerged as crucial technologies for enhancing the security and efficiency of campus networks. VLANs allow network administrators to logically divide the physical network into smaller, isolated segments, improving security and network management (Putri et al., 2023). Network administrators can apply different security policies and control access to sensitive network resources by grouping users and devices with the same security requirements into separate VLANs.

VLANs offer several security benefits for computer networks, including isolating network traffic between different segments, limiting the impact of security incidents, and preventing attackers from accessing the entire network. Additionally, VLANs enable network administrators to control access to network resources based on VLAN membership, ensuring that only authorized users can access sensitive data and applications.

Internet security is of utmost importance and should not be taken lightly, considering the various risks that may arise, including sniffing. This activity can cause significant damage, ranging from the theft of personal data to unauthorized access to certain accounts. Tools like Wireshark can help identify vulnerabilities in insecure protocols, such as HTTP, and emphasize the importance of using more secure protocols like HTTPS (Anwar, 2024). Network security vulnerabilities can pose serious risks to businesses and educational institutions. Poorly managed vulnerabilities can have severe consequences for businesses and users, including data loss, system breaches, or operational disruptions, resulting in financial and reputational losses (Fauzan Asrin et al., 2024). Sensitive data, such as employees, staff, and student's personal information and operational data, can become targets for parties seeking to exploit security gaps (Aman, 2023). One possible threat is a Man-in-the-Middle (MitM) attack, where an intruder can observe or alter communication between devices on the network without permission (Fairuzabadi et al., 2023).

This study investigates the implementation of VLANs to enhance communication security in campus network environments. It focuses on designing and implementing a multi-VLAN network, examining its effectiveness in protecting sensitive communication from unauthorized access. The research explores two scenarios: First, the Legitimate User scenario analyzes how legitimate users can securely access servers within a multi-VLAN network. The second scenario, the Attacker scenario, aims to investigate how potential attackers might attempt to intercept communications and evaluate the effectiveness of VLAN security measures in preventing unauthorized access. By examining these scenarios, this study aims to provide practical insights into applying VLANs for enhancing campus network security and protecting sensitive communications from cyber threats.

2. Literature Review

Existing literature provides valuable insights into the benefits and applications of VLAN technology in campus and library networks. Based on research and testing conducted on network security simulations using the Network Development Life Cycle method with Switch Port Security at PT Pinus Merah Abadi, it can be concluded that configuring switch port security with sticky port security settings is the most effective method. This approach allows for automatic registration of MAC addresses and disconnects unknown devices, thereby enhancing network security. Additionally, DoS attacks cause a decline in CPU performance and increased memory usage on devices connected to the network, leading to operational disruptions within the company (Putri et al., 2023).

To address cybercrime, Indonesia needs to involve technology experts, strengthen defense industry cooperation, and develop a cyber defense system supported by proper regulations and a cyber command center. Furthermore, strong information risk management and legal support are required to protect confidential data and bolster national defense (Soesanto et al., 2023). Research on network security system simulations shows that combining Snort IPS and Honeypot Artillery is effective in detecting and preventing network attacks. Combining these systems is considered adequate for improving network security but requires enhancements by adding local rules in Snort, updating rules, and improving server performance (Aminanto & Sulistyo, 2020). Investigating ARP Spoofing attacks using the TAARA method successfully identified evidence of attacks through router-side analysis. Wireshark proved superior to Network Miner Free in detecting these attacks (Wijayanto, 2023). Research on ARP and DNS attacks using the NIST forensic method with Bettercap in Kali Linux showed that Wireshark effectively detects abnormal network traffic and identifies ARP and DNS spoofing attacks [16-21]. These findings emphasize the importance of network monitoring and forensic analysis and the need for strong cybersecurity strategies to prevent future attacks (Prakoso & Khamas Heikmakhtiar, 2024). Research using Packet Tracer to design PT's VLAN Trunking Protocol (VTP) network infrastructure. Rukun Sejahtera Teknik indicated that VTP client switches cannot modify VLANs from the VTP server switch, and PCs cannot access different VLANs (Ar-Rasyid et al., 2024).

Research on data sniffing in WiFi networks showed that Wireshark can reveal critical information such as usernames and passwords from websites using the HTTP protocol. Data sniffing can be mitigated by using HTTPS for data encryption and avoiding untrusted WiFi networks (Khaerullah & Mustafa, 2024). This study aims to analyze and design computer networks using the VLAN concept, which allows network segmentation into several groups based on needs. The PPDIOO method is used in this research, from preparation to network optimization. Simulations are conducted using Cisco Packet Tracer version 7.2 (Br Sipayung et al., 2024). In this study, we will explore the implementation of VLAN-based network architecture, focusing on two specific scenarios to illustrate the benefits of secure communication and the challenges faced by potential attackers.

2.1 VLAN

A Virtual Local Area Network (VLAN) is a method for dividing a network into several smaller segments (Revansa et al., 2022). VLAN's primary goal is to reduce broadcast traffic on each subnet, improving information traffic efficiency. Thus, VLAN functions to enhance overall network performance. Additionally, a Top-Down approach is often used in network planning, where strategic decisions for network construction are based on the computer needs and facilities required by the entire unit within an organization.

2.2 Webservice

A web service is generally an application that utilizes the internet to access standard protocols and store data in JSON or XML format (Ramadan et al., 2021). This allows the data to be accessed by other systems, even if there are differences in platform, operating system, or programming language.

2.3 ARPSpoffing

ARP Spoofing attacks are a type of spoofing attack that can trigger further attacks. This technique exploits vulnerabilities in the ARP protocol (June et al., 2017). Analyzing ARP Spoofing attacks from the router side and using sniffers to capture network traffic can help investigators obtain relevant evidence of such attacks. Persistent attacks can involve reading traffic through Man-in-the-Middle (MitM) attacks and network denial using Denial of Service (DoS) techniques (Wijayanto, 2023).

3. Conceptual Framework

Data was collected through network simulations built using VirtualBox, where scenarios of server access by a Nice Guy and eavesdropping by a Bad Guy were tested using HTTP and HTTPS protocols. The research methodology used in this study follows the PPDIOO model (Prepare, Plan, Design, Implement, Operate, and Optimize) (Br Sipayung et al., 2024). model PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) (Br Sipayung et al., 2024).

The planning phase begins with a literature review and gathering references from relevant journals to understand the operation and requirements of network systems, ensuring they can be implemented as expected. Following this, the preparation phase involves mapping system needs, such as the software and network configurations required to support VLAN implementation and network security. At this stage, planning and preparation are carried out simultaneously, as they are interrelated and form a critical foundation that must be addressed to ensure that subsequent stages are conducted in a more focused and effective manner. This study starts with a comprehensive review of relevant literature and industry best practices to establish a strong basis for the research. Additionally, the researchers have set up a virtual network environment using VirtualBox to simulate the proposed network architecture, including implementing routers, servers, and client devices within the VLAN structure. The Research Stages can be seen in Figure 1.

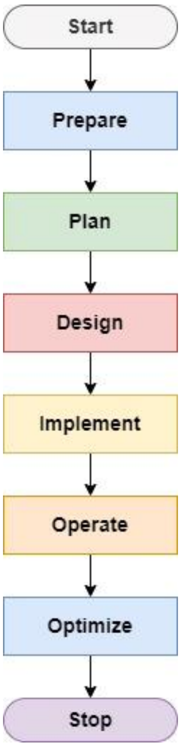


Figure 1. Research Stages

Activities were conducted on network operations, focusing primarily on how data is transmitted and whether there were any attempts at eavesdropping or data manipulation by the Bad Guy. The fundamental concept used in this research is that VLANs can be employed to segregate different types of devices within a network, and protocols such as HTTPS are necessary to protect data from eavesdropping.

3.1 System Design

The virtual network design includes several devices, such as routers, switches, servers, and clients, arranged in two different VLANs. The Nice Guy and Bad Guy are in the same VLAN, while the server is in a separate VLAN. Network Topology Design can be seen in Figure 2.

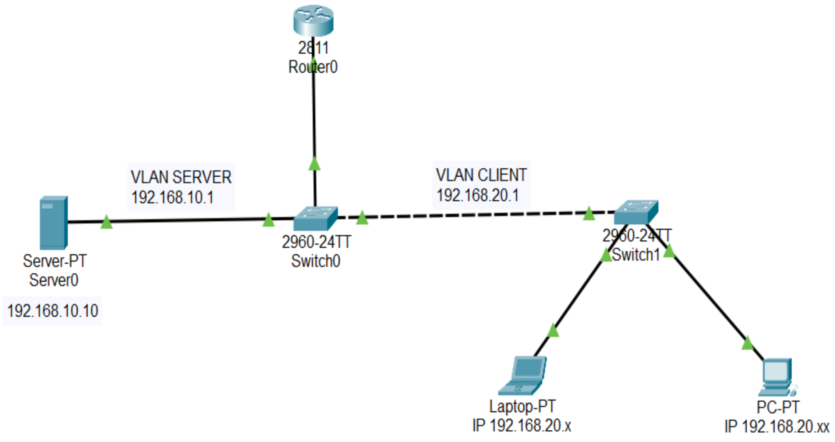


Figure 2. Network Topology Design

3.2 Centralization Model

Several key components play a crucial role in maintaining security and data transmission efficiency in the designed network architecture. The Nice Guy, as a client, is connected to the CLIENT VLAN, which isolates client devices from other networks, ensuring more secure access. This client accesses the Server through a Router, which acts as a bridge between the CLIENT VLAN and the SERVER VLAN, ensuring proper routing between the two. The HTTPS protocol is used to protect the transmitted data, securing the communication between the client and the server.

The SERVER VLAN stores critical organizational data and isolates the server from the client and other networks. The server receives requests from the Nice Guy and sends data back using the HTTPS protocol, ensuring data security during transmission. All traffic between the client and the server is monitored by the Network Monitoring System, which is responsible for detecting and preventing data breaches and unauthorized access, thereby maintaining the integrity and confidentiality of the transmitted data. A diagram of Client Communicating with Server through Router can be seen in Figure 3.

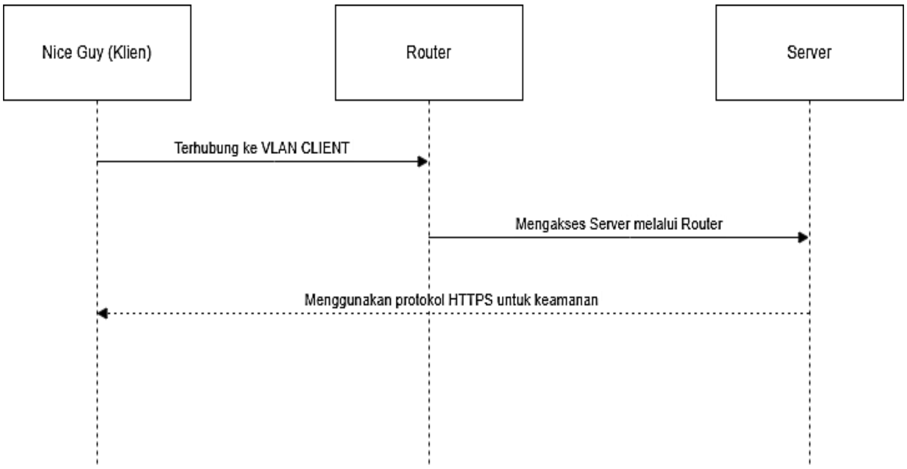

Nice Guy (Klien)
Router
Server
Terhubung ke VLAN CLIENT
Mengakses Server melalui Router
Menggunakan protokol HTTPS untuk keamanan

Figure 3. Diagram of Client Communicating with Server through Router

Table 1. Software Requirements

Type	Version	Description
Kali Linux	2023.2	Client Bad Guy
Debian	10	OS Server
Debian	10	OS Router
Wireshark	4.2.6	Records network traffic
Virtualbox	6.0	Virtualization of scenarios
XAMPP	V3.2.4	To implement HTTP and HTTPS scenarios

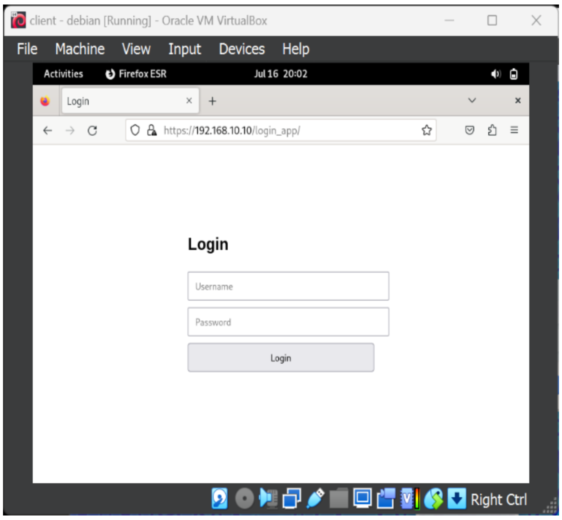
This study includes 2 scenarios: the Nice Guy and the Bad Guy. We use several network devices, such as routers, servers, and clients, to implement these scenarios. The software or tools needed to build the system are as follows the Table 1.

3.3 Virtual Network Creation

The virtual network is created using VirtualBox, with the operating systems serving as the router, server, and clients. Configuration is performed to ensure that the router supports VLAN and DHCP Server in each VLAN. The server and clients are set to receive IP addresses from the router, with the server located in the SERVER VLAN and clients in the CLIENT VLAN.

The router connects the two different VLANs: SERVER VLAN and CLIENT VLAN. Switch 0 manages the SERVER VLAN, where the server and the Web Server service are located. Switch 1 manages the CLIENT VLAN, where clients, including legitimate users (Nice Guy) and attackers (Bad Guy), are located. The server in the SERVER VLAN has the IP address 192.168.10.10, where the Web Server service is hosted. The Bad Guy and Nice Guy are in the CLIENT VLAN with IP addresses of 192.168.20.x.

Scenario 1: Legitimate User Accesses Server Securely (Nice Guy Scenario), in this scenario, a legitimate user (Nice Guy) connects to the CLIENT VLAN with the IP address 192.168.20.10 and attempts to access the web server located in the SERVER VLAN with the IP address 192.168.10.10. Login Display Menu can be seen in Figure 4.


client - debian [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Firefox ESR
Jul 16 20:02
Login
https://192.168.10.10/login_app/
Right Ctrl

Login

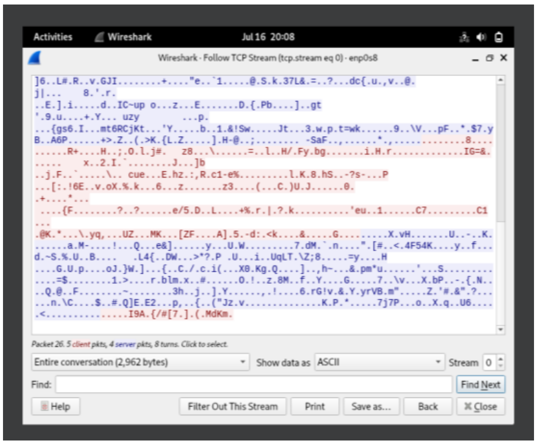
Username

Password

Login

Figure 4. Login Menu Display

Communication between the Nice Guy and the server is expected to be secure, using the HTTPS protocol to prevent unauthorized eavesdropping or data manipulation. In this scenario, the Nice Guy successfully accesses the server using HTTPS. The data transmitted between the client and the server is encrypted, preventing the attacker (Bad Guy) in the same VLAN from intercepting or obtaining useful information. Wireshark TCP Follow Display HTTPS is shown in Figure 5.



```
]6..L#.R..v.GJI........+...."e..`1.....@.S.k.37L&.=..?...dc{.u.,v..@.
j|...    8.'.r.
..E.].i.....d..IC~up o...z...E.......D.{.Pb....]..gt
'.9.u....+.Y... uzy        ...p.
...{gs6.I...mt6RCjKt...'Y.....b..1.&!Sw.....Jt...3.w.p.t=wk......9..\V...pF..*.$7.y
B..A6P......+>.Z..(.>K.{L.Z.....].H-@..;........ -SaF..,......*.,.............8....
......R+....H..;.O.l.j#.   z8...\......=..l..H/.Fy.bg.......i.H.r.............IG=&.
.....    x..2.I.`........J...]b
..j.F..`.....\.. cue...E.hz.:,R.c1-e%.........l.K.8.hS..-?s-...P
...[:.!6E..v.oX.%.k...6...z.......z3....(...C.)U.J......0.
.+....*...
 ....{F........?..?......e/5.D..L....+%.r.|.?.k..........'eu..1......C7.........C1
...
.@K.*...\.yq,...UZ...MK...[ZF....A].5.-d:.<k....&.....G.........X.vH.......U..-..K.
.......a.M-....!...Q...e&]......y...U.W.........7.dM.`.n....".[#..<.4F54K....y..f...
d.~S.%.U..B....   .L4{..DW...>*?.P .U...i..UqLT.\Z;8.....=y....H
....G.U.p....oJ.}W.]...{..C./.c.i(...X0.Kg.Q....]..,h~...&.pm*u......'...S.........
....=$........1.>....r.blm.x..#......O.!..z.8M..f..Y....G.....7..\v...X.bP..-.{.N..
..Q.@..F........~........3h..j..].Y......,.!....6.rG!v.&.Y.yrVB.m".....Z.'#.&".?...
...n.\C....$..#.Q]E.E2...p,..{..("Jz.v..............K.P.*.....7j7P...o..X.q..U6....
.<................I9A.{/#[7.].(.MdKm.
```

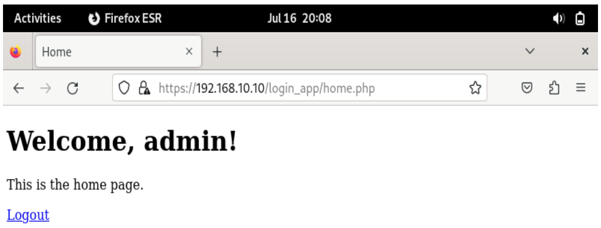
Packet 26. 5 client pkts, 4 server pkts, 8 turns. Click to select.

Entire conversation (2,962 bytes) Show data as ASCII Stream 0

Find:

Figure 5. Wireshark TCP Follow Display HTTPS

HTTPS is effective in protecting communication and ensuring data security within the VLAN. It can be observed that the router can monitor the data requested from the client to the server, as the traffic must pass through the router. The yellow highlight indicates the server replying to the client request on port 443, which is used for SSL, ensuring encrypted data transmission. Furthermore, from the router, we attempt to follow the TCP stream to obtain the password inputted by the client (Good Guy). Since the data transmitted is encrypted with SSL, it will only display random text strings. Thus, the client can securely access the server. Admin Page Display with HTTPS as shown in Figure 6.



Welcome, admin!

This is the home page.

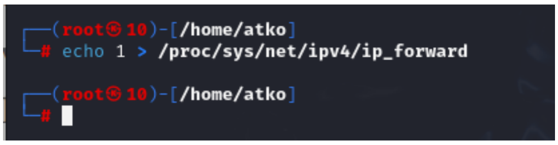
Logout

Figure 6. Admin Page Display with HTTPS

Scenario 2: Attacker Attempts to Eavesdrop on Communication (Bad Guy Scenario)

First, the Bad Guy needs to set up before attacking the target. The initial step is to use `nmap` to scan for clients available within the VLAN. Using `nmap -sn 192.168.20.0/24`, we see 192.168.20.11 and 192.168.20.10, with 192.168.20.11 being the IP of the Bad Guy himself. After obtaining the target IP, the next step is to perform ARP Spoofing, a technique used to redirect network traffic intended for a specific device, such as a router, to a device controlled by the attacker. ARP Spoofing exploits the ARP (Address Resolution Protocol), which maps IP addresses to MAC addresses in the local network. Use `apt-get install dsniff` to install the necessary tools.

Before proceeding with ARP Spoofing, activate IP forwarding on the Bad Guy's machine to allow it to forward IP packets. IP forwarding turns on or off the system's ability to forward network packets between different network interfaces. Enabling IP forwarding allows the system to function as a router, forwarding packets from one network interface to another, as shown in Figure 7.

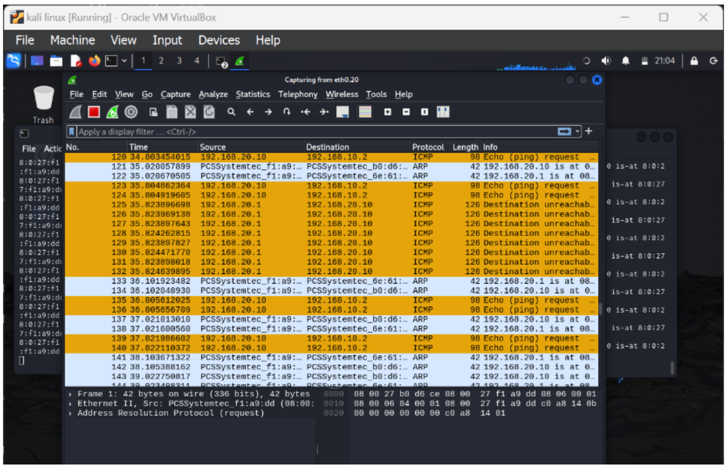


```
┌──(root㉿10)-[/home/atko]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿10)-[/home/atko]
└─# █
```

Figure 7. Activating IP Forwarding

Type the command `sudo arpspoof -i eth0.20 -t 192.168.20.10 -r 192.168.20.1` to deceive the "Nice Guy" (192.168.20.10) into thinking that the attacker (Bad Guy) is the gateway (192.168.20.1), so traffic from the "Nice Guy" to the gateway will be redirected to the attacker. Type the command `sudo arpspoof -i eth0 -t 192.168.20.1 -r 192.168.20.10` to deceive the gateway (192.168.20.1) into thinking that the attacker (Bad Guy) is the "Nice Guy" (192.168.20.10), so traffic from the gateway to the "Nice Guy" will be redirected to the attacker, as shown in Figure 8.

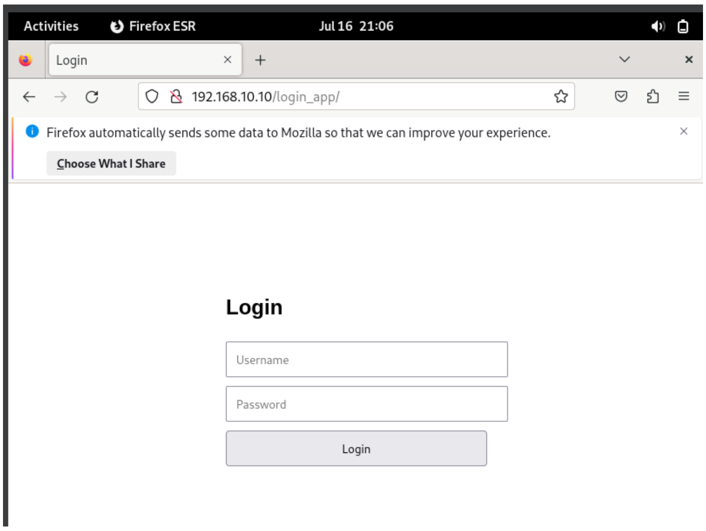

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
Capturing from eth0.20
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source                Destination           Protocol Length Info
  120 34.803454015  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  121 35.020057899  PCSSystemtec_f1:a9:…  PCSSystemtec_b0:d6:…  ARP        42 192.168.20.10 is at 0…
  122 35.020670505  PCSSystemtec_f1:a9:…  PCSSystemtec_6e:61:…  ARP        42 192.168.20.1 is at 08…
  123 35.804862364  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  124 35.804919605  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  125 35.823896698  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  126 35.823969138  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  127 35.823897643  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  128 35.824262815  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  129 35.823897827  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  130 35.824471778  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  131 35.823898018  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  132 35.824639895  192.168.20.1          192.168.20.10         ICMP      126 Destination unreachab…
  133 36.101923482  PCSSystemtec_f1:a9:…  PCSSystemtec_6e:61:…  ARP        42 192.168.20.1 is at 08…
  134 36.102048930  PCSSystemtec_f1:a9:…  PCSSystemtec_b0:d6:…  ARP        42 192.168.20.10 is at 0…
  135 36.805612025  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  136 36.805656709  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  137 37.021013010  PCSSystemtec_f1:a9:…  PCSSystemtec_b0:d6:…  ARP        42 192.168.20.10 is at 0…
  138 37.021600560  PCSSystemtec_f1:a9:…  PCSSystemtec_6e:61:…  ARP        42 192.168.20.1 is at 08…
  139 37.821986602  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  140 37.822110372  192.168.20.10         192.168.10.2          ICMP       98 Echo (ping) request  …
  141 38.103671322  PCSSystemtec_f1:a9:…  PCSSystemtec_6e:61:…  ARP        42 192.168.20.1 is at 08…
  142 38.105388162  PCSSystemtec_f1:a9:…  PCSSystemtec_b0:d6:…  ARP        42 192.168.20.10 is at 0…
  143 39.022750817  PCSSystemtec_f1:a9:…  PCSSystemtec_b0:d6:…  ARP        42 192.168.20.10 is at 0…

› Frame 1: 42 bytes on wire (336 bits), 42 bytes    0000  08 00 27 b0 d6 ce 08 00  27 f1 a9 dd 08 06 00 01
› Ethernet II, Src: PCSSystemtec_f1:a9:dd (08:00:   0010  08 00 06 04 00 01 08 00  27 f1 a9 dd c0 a8 14 0b
› Address Resolution Protocol (request)             0020  00 00 00 00 00 00 c0 a8  14 01
```

Figure 8. Network Tracking Display in Wireshark

Ensure both `arpspoof` commands are running simultaneously. Next, if we try to ping the server from the "Nice Guy" side, we will see that the IP is first redirected to the Bad Guy before reaching the router. Then, we can use Wireshark on the Bad Guy to monitor network traffic from the "Nice Guy" and follow the network activity from the "Nice Guy." After that, if the "Nice Guy" tries to access HTTP, as shown in Figure 9.

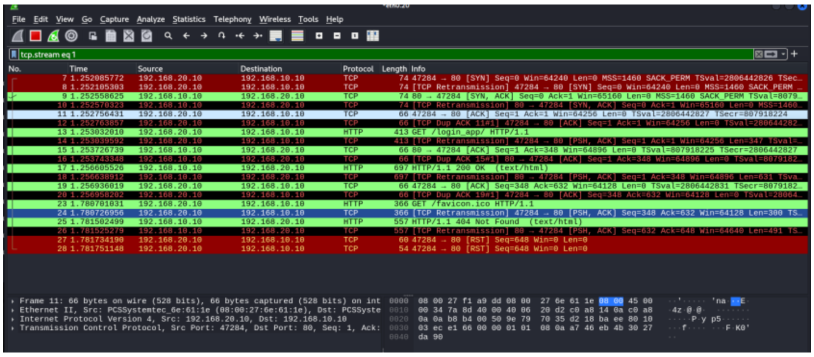


Firefox automatically sends some data to Mozilla so that we can improve your experience.

Figure 9. Login Page from the Nice Guy's Side

The Bad Guy can be observed when the user attempts to access 192.168.10.10 using HTTP. When trying to follow the TCP stream, we find the password input by the Nice Guy because the username and password are not encrypted. It can be seen that the username and password entered by the Nice Guy are Username: admin and Password: admin123.

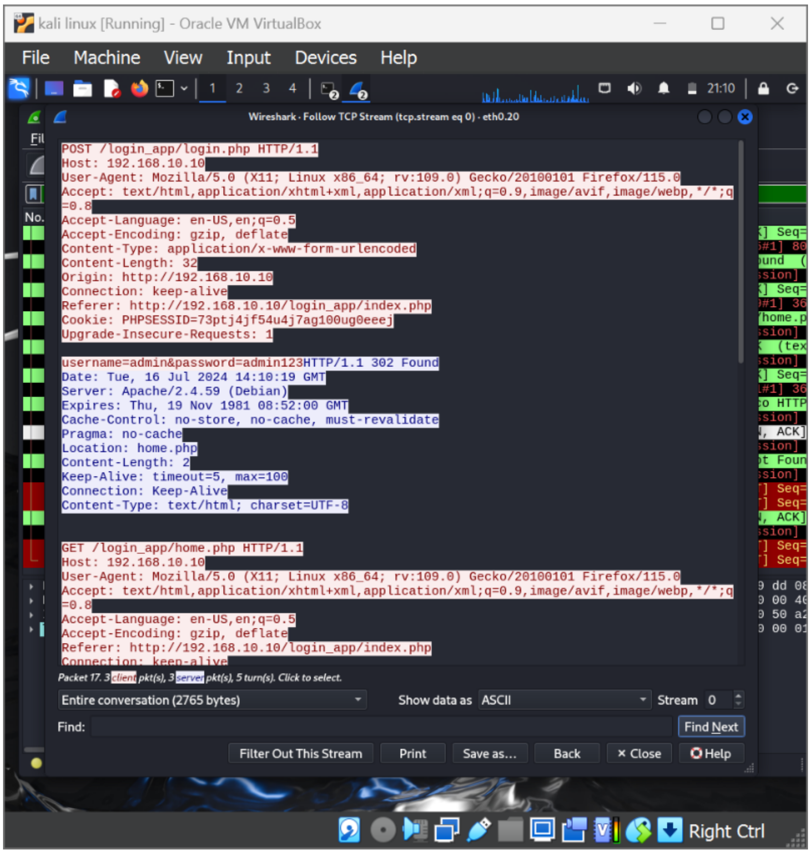
Figure 10. In this scenario, an attacker (Bad Guy) is connected to the same VLAN Client with the IP address 192.168.20.11. The attacker attempts to intercept communication between the Nice Guy and the web server using packet monitoring tools such as Wireshark, as shown in Figures 10 and 11.


*eth0.20
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1

```
No.   Time          Source          Destination     Protocol Length Info
    7 1.252085772   192.168.20.10   192.168.10.10   TCP      74 47284 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2806442826 TSec…
    8 1.252105303   192.168.20.10   192.168.10.10   TCP      74 [TCP Retransmission] 47284 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM …
    9 1.252558625   192.168.10.10   192.168.20.10   TCP      74 80 → 47284 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=8079…
   10 1.252570323   192.168.10.10   192.168.20.10   TCP      74 [TCP Retransmission] 80 → 47284 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460…
   11 1.252756431   192.168.20.10   192.168.10.10   TCP      66 47284 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2806442827 TSecr=807918224
   12 1.252763857   192.168.20.10   192.168.10.10   TCP      66 [TCP Dup ACK 11#1] 47284 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=280644282…
   13 1.253032010   192.168.20.10   192.168.10.10   HTTP    413 GET /login_app/ HTTP/1.1
   14 1.253039592   192.168.20.10   192.168.10.10   TCP     413 [TCP Retransmission] 47284 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=347 TSval=…
   15 1.253726739   192.168.10.10   192.168.20.10   TCP      66 80 → 47284 [ACK] Seq=1 Ack=348 Win=64896 Len=0 TSval=807918225 TSecr=2806442827
   16 1.253743348   192.168.10.10   192.168.20.10   TCP      66 [TCP Dup ACK 15#1] 80 → 47284 [ACK] Seq=1 Ack=348 Win=64896 Len=0 TSval=8079182…
   17 1.256605526   192.168.10.10   192.168.20.10   HTTP    697 HTTP/1.1 200 OK  (text/html)
   18 1.256638912   192.168.10.10   192.168.20.10   TCP     697 [TCP Retransmission] 80 → 47284 [PSH, ACK] Seq=1 Ack=348 Win=64896 Len=631 TSva…
   19 1.256936019   192.168.20.10   192.168.10.10   TCP      66 47284 → 80 [ACK] Seq=348 Ack=632 Win=64128 Len=0 TSval=2806442831 TSecr=8079182…
   20 1.256958202   192.168.20.10   192.168.10.10   TCP      66 [TCP Dup ACK 19#1] 47284 → 80 [ACK] Seq=348 Ack=632 Win=64128 Len=0 TSval=28064…
   23 1.780701031   192.168.20.10   192.168.10.10   HTTP    366 GET /favicon.ico HTTP/1.1
   24 1.780726956   192.168.20.10   192.168.10.10   TCP     366 [TCP Retransmission] 47284 → 80 [PSH, ACK] Seq=348 Ack=632 Win=64128 Len=300 TS…
   25 1.781502499   192.168.10.10   192.168.20.10   HTTP    557 HTTP/1.1 404 Not Found  (text/html)
   26 1.781525279   192.168.10.10   192.168.20.10   TCP     557 [TCP Retransmission] 80 → 47284 [PSH, ACK] Seq=632 Ack=648 Win=64640 Len=491 TS…
   27 1.781734190   192.168.20.10   192.168.10.10   TCP      60 47284 → 80 [RST] Seq=648 Win=0 Len=0
   28 1.781751148   192.168.20.10   192.168.10.10   TCP      54 47284 → 80 [RST] Seq=648 Win=0 Len=0

› Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on int   0000  08 00 27 f1 a9 dd 08 00  27 6e 61 1e 08 00 45 00   ··'·····'na···E·
› Ethernet II, Src: PCSSystemtec_6e:61:1e (08:00:27:6e:61:1e), Dst: PCSSyste   0010  00 34 7a 8d 40 00 40 06  20 d2 c0 a8 14 0a c0 a8   ·4z·@·@· ·······
› Internet Protocol Version 4, Src: 192.168.20.10, Dst: 192.168.10.10          0020  0a 0a b8 b4 00 50 9e 79  70 35 d2 18 ba ee 80 10   ·····P·y p5······
› Transmission Control Protocol, Src Port: 47284, Dst Port: 80, Seq: 1, Ack:   0030  03 ec e1 66 00 00 01 01  08 0a a7 46 eb 4b 30 27   ···f···· ···F·K0'
                                                                               0040  da 90                                              ··
```

Figure 10. Wireshark TCP Follow Display HTTP


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
21:10
Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0.20
Fil
No.
Right Ctrl

```
POST /login_app/login.php HTTP/1.1
Host: 192.168.10.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://192.168.10.10
Connection: keep-alive
Referer: http://192.168.10.10/login_app/index.php
Cookie: PHPSESSID=73ptj4jf54u4j7ag100ug0eeej
Upgrade-Insecure-Requests: 1

username=admin&password=admin123HTTP/1.1 302 Found
Date: Tue, 16 Jul 2024 14:10:19 GMT
Server: Apache/2.4.59 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: home.php
Content-Length: 2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


GET /login_app/home.php HTTP/1.1
Host: 192.168.10.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.10.10/login_app/index.php
Connection: keep-alive
```

Packet 17. 3 client pkt(s), 3 server pkt(s), 5 turn(s). Click to select.

Entire conversation (2765 bytes) Show data as: ASCII Stream: 0

Figure 11. Wireshark TCP Follow Display HTTP

The main focus is determining if the attacker can successfully capture sensitive information when the Nice Guy uses the insecure HTTP protocol. Like the Nice Guy, the Bad Guy is connected to the VLAN Client. The Bad Guy uses Wireshark's packet monitoring tool to capture data packets in the VLAN Client. The Nice Guy attempts to access the web server using HTTP. The Bad Guy tries to intercept the communication and extract sensitive information such as usernames and passwords. In this scenario, when the Nice Guy accesses the server using HTTP, the Bad Guy successfully intercepts the communication and obtains sensitive data such as usernames and passwords. This demonstrates that using the unencrypted HTTP protocol exposes a serious security vulnerability, where an attacker in the same VLAN can easily access confidential information.

The results of the HTTP and HTTPS scenario tests demonstrate the differences between the two scenarios. The HTTPS scenario successfully encrypts communication between the Nice Guy and the web server. Data transmitted over the network cannot be accessed by the Bad Guy, who cannot capture meaningful information even though they are in the same VLAN. The encryption provided by HTTPS effectively secures communication, highlighting the importance of using secure protocols in VLAN environments. When the Nice Guy accesses the server using HTTP, the Bad Guy successfully intercepts the communication and captures sensitive data, including the Nice Guy's username and password. The lack of encryption in HTTP makes the data vulnerable to interception, emphasizing the critical security risks associated with using insecure communication protocols.

The results from both scenarios underscore the need to implement secure communication protocols, such as HTTPS, in VLAN-based networks to protect against potential attacks and unauthorized access. The VLAN architecture and secure protocols provide a robust framework for managing and safeguarding network communication. The findings indicate that when the Nice Guy accesses the server via HTTPS, the Bad Guy cannot intercept the transmitted data due to SSL/TLS encryption. Conversely, when the Nice Guy uses HTTP, the Bad Guy can easily intercept data, including usernames and passwords, through techniques such as ARP Spoofing and Wireshark packet analysis. This underscores the importance of using secure protocols to prevent security threats.

5. Conclusion

The results from these scenarios highlight the importance of using secure protocols such as HTTPS in VLAN networks to protect communication from eavesdropping and other attacks. While VLANs provide network segmentation and security, using unencrypted protocols like HTTP still poses significant risks, where attackers can easily access sensitive data. Future research could explore additional security measures, such as implementing firewall rules, intrusion detection systems (IDS), and advanced encryption methods to enhance VLAN-based network security. Furthermore, developing more complex simulations with diverse network topologies and broader attack vectors could offer deeper insights into the strengths and weaknesses of VLAN environments across various settings.

Acknowledgments: Thanks to all those who helped in this research process, thanks to Politeknik Negeri Pontianak, hopefully this research can be a good reference. and can be developed properly and expand similar knowledge in the field of Network security.

Author contributions: All authors are responsible for building Conceptualization, Methodology, analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision of project administration, funding acquisition, and have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aman, A. (2023). Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ. Digital Transformation Technology, 3(2), 824–831. https://doi.org/10.47709/digitech.v3i2.3378
2. Aminanto, A., & Sulistyo, W. (2020). Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery. Aiti, 16(2), 135–150. https://doi.org/10.24246/aiti.v16i2.135-150
3. Anwar, A. N. (2024). MALCOM: Indonesian Journal of Machine Learning and Computer Science Network Security Analysis on The Internet Facility (Wifi) UIN Syarif Hidayatullah Jakarta Against Packet Sniffing Attacks. 4(3), 771–776.
4. Ar-Rasyid, H., Broto, S., & Artika, W. (2024). Optimasi Infrastruktur Jaringan Vlan Trunking Protocol Menggunakan Simulasi Packet Tracer Pada Pt. Rukun Sejahtera Teknik. Jeis: Jurnal Elektro Dan Informatika Swadharma, 4(1), 39–46. https://doi.org/10.56486/jeis.vol4no1.422

5. Br Sipayung, P. I. O., Purba, V., & Agussalim, A. (2024). Analisis, Perancangan, dan Simulasi Jaringan VLAN Menggunakan Metode PPDIOO (Studi Kasus: SMAS Santo Yusup Surabaya). TeknoIS : Jurnal Ilmiah Teknologi Informasi Dan Sains, 14(1), 110–118. https://doi.org/10.36350/jbs.v14i1.237
6. Fairuzabadi, M., Pangaribuan, J. J., Moedjahedy, J. H., Sihotang, J. I., Simarmata, J., Andryanto, A., … others. (2023). Keamanan Sistem Informasi dan Kriptografi. Yayasan Kita Menulis.
7. Fauzan Asrin, S.Kom., M.Kom., Ismarmiaty, ST., MMSI. Dr. Si Arie Setya Putra, CA., M.T.I., Nuk Ghurroh Setyoningrum, S.Kom, M. C. ., Ade Yuliana, S.T., M.T., Juwari, S.Kom., M. K. ., Tati Ernawati, M.T. , Agni Isador Harsapranata, S.Kom., M.M., M. K., & Alfa Saleh, M.Kom., Novi Aryani Fitri, S.T., M.Tr.Kom. Putri Ariatna Alia, S.ST., M.T. , Nia Ekawati, S.Kom., M. SI. Etza Nofarita, ST., M.Kom., Dr. Ir. Iwan Setiawan, M. (2024). Keamanan Sistem Informasi. PT Penamuda Media.
8. June, M., No, I., & Bijral, R. K. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. International Journal of Advanced Research in Computer Science, 8(5), 2074–2077. http://www.ijarcs.info/index.php/Ijarcs/article/view/4016/3667
9. Khaerullah, S. M., & Mustofa, D. (2024). Penggunaan Wireshark Dalam Penyadapan Lalu Lintas Data Berprotokol Http Pada Jaringan Wi-Fi. Jurnal Ilmiah IT CIDA, 10(1), 19. https://doi.org/10.55635/jic.v10i1.203
10. Prakoso, G., & Khamas Heikmakhtiar, A. (2024). Analisis Keamanan Jaringan: ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology. Journal on Education, 06(02), 12895–12902.
11. Putri, R. M., Zulkifli, Z., & Fajri, R. M. (2023). Simulasi Keamanan Jaringan Dengan Metode Network Development Life Cycle Menggunakan Switch Port Security Pada Pt, Journal of Intelligent Networks and IoT, 107–115. http://www.repository.uigm.ac.id/id/eprint/380/1/RaMartasyaPutri_2019310071_file cover-Daftar isi-1.pdf
12. Ramadan, A. R., Prakoso, A. W., & Dwi C, G. (2021). Implementasi Kriptografi AES untuk Keamanan Pengiriman Data Internet of Things Menggunakan Web Service Rest pada NodeMCU. Systemic: Information System and Informatics Journal, 6(1), 1–6. https://doi.org/10.29080/systemic.v6i1.752
13. Revansa, E., Yohanes, S. B., & Petrus, K. (2022). Perancangan Jaringan Virtual Local Area Network (Vlan) Untuk Menunjang Transaksi Data Antar Jaringan. Jurnal Teknologi Informasi, 6(1), 102–111.
14. Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen, 1(2), 186.
15. Wijayanto, A. (2023). Forensik Jaringan Terhadap Serangan Arp Spoofing Menggunakan Metode Taara. ijay. https://dspace.uii.ac.id/handle/123456789/42627
16. F. Mvah, V. K. Tchendji, C. T. Djamegni, A. H. Anwar, D. K. Tosh and C. Kamhoua, "Deception-Based IDS Against ARP Spoofing Attacks in Software-Defined Networks," 2024 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2024, pp. 188-192, doi: 10.1109/ICNC59896.2024.10556188.
17. D. Patel and D. Shah, "Combating ARP Spoofing: Detection and Analysis Techniques," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 543-547, doi: 10.23919/INDIACom61295.2024.10498305.
18. D. R. Thomas, P. V, W. Nancy, G. Sowmiya, A. T. P and V. Peroumal, "Detection and Prevention of Poisoning Targets with ARP Cache using Scapy," 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/IITCEE59897.2024.10467270.
19. Y. A. Mohamed, M. Hashim and M. Bashir, "A Strategy to Mitigate ARP Spoofing Attacks on Hypervisors," 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2024, pp. 1-8, doi: 10.1109/ICAECT60202.2024.10469115.

20. Q. A. Al-Haija, Z. Masoud, A. Yasin, K. Alesawi and Y. Alkarnawi, "Revolutionizing Threat Hunting in Communication Networks: Introducing a Cutting-Edge Large-Scale Multiclass Dataset," 2024 15th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2024, pp. 1-5, doi: 10.1109/ICICS63486.2024.10638287.
21. K. U. Aditya, P. N. Kamath, Y. Poral, B. D. Mallika and V. Acharya, "Framework for Early Cyber Attack Detection Using ML Models Deployed On Fog Devices," 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 2024, pp. 1-6, doi: 10.1109/ISDFS60797.2024.10527351.