International Journal of Engineering and Computer Science Applications (IJECSA)
Vol. 4, No. 1, March 2025, pp. 1∼12
ISSN: 2828-5611
DOI: doi.org/10.30812/ijecsa.v4i1.4784

Analyze Threats in a Virtual Lab Network Using Live Forensic Methods on MetaRouter

Firmansyah, Bayu Wibisana, Muhammad Jordan
Universitas Islam Al-Azhar, Mataram, Indonesia

Article Info

Article history:

Received January 04, 2025
Revised January 18, 2025
Accepted January 21, 2025

Keywords:

Live Forensic
Metarouter
Threats
Virtual Lab

ABSTRACT

This research identified critical network anomalies in the MetaRouter virtual environment, focusing on Internet Protocol (IP) activity related to routers, networks, and client devices. Suspicious interactions were observed between IP 192.168.1.100 (router) and IP 172.16.205.53 (client), including reused Transmission Control Protocol (TCP) port numbers and incomplete synchronize (SYN) sessions, indicating potential spoofing attempts. Invalid route information involving 192.168.1.100 highlights malicious modifications to the routing table, indicating an attempt to manipulate the routing information. Packet inconsistencies, such as "TCP Previous segment not captured" and "Spurious Retransmission," revealed interference between the client and router, possibly caused by an external attacker exploiting network protocol vulnerabilities. This research aims to analyze threats in virtual lab networks using live forensic methods on MetaRouter to detect anomalies, focusing on Border Gateway Protocol (BGP) and TCP deviations in MetaRouter. This research method is a controlled prototype experimental setup in a virtual laboratory consisting of two routers and two client devices. This method simulates real-world network operations to identify malicious activities. Wireshark is used for real-time packet-level monitoring and analysis because it has powerful visualization and filtering capabilities, surpassing tools like tcpdump. This research integrates live forensic techniques to collect and analyze routing logs, packet data, and protocol behavior. The results of this research are the identification of suspicious behaviors, such as reused TCP port numbers, incomplete SYN sessions, and unauthorized route announcements, indicating potential spoofing and BGP hijacking attempts. Packet data irregularities, including "Out-Of-Order" messages and abrupt session terminations, are also detected, revealing disruptions in traffic flow caused by malicious activities. The results of this research highlight the effectiveness of the forensic framework in identifying and documenting network anomalies in virtual environments, which have significant implications for improving security in cloud-based and hybrid networks. This research provides a scalable and replicable methodology that can improve real-time anomaly detection and response, paving the way for future advances in network security.

Corresponding Author:

Firmansyah, +6281802628765,
Universitas Islam Al-Azhar, Mataram, Indonesia,
Email: f.firman@unizar.ac.id

How to Cite: F. Firmansyah, B. Wibisana, and M. Jordan, "Analyze Threats in a Virtual Lab Network Using Live Forensic Methods on MetaRouter," *International Journal of Engineering and Computer Science Applications (IJECSA)*, vol. 4, no. 1, pp. 1-12, Mar. 2025. doi: doi.org/10.30812/ijecsa.v4i1.4784.

1. INTRODUCTION

The adoption of virtualization technology has significantly increased in recent years [1]. Virtualization enables a single physical server to host multiple virtual machines, maximizing the utilization of physical resources such as CPU, RAM, and storage. This allows multiple applications or operating systems to run on a single physical server. By leveraging virtualization, organizations can reduce the number of physical servers required, lower maintenance costs, save physical space, and improve energy efficiency [2]. Cybersecurity threats have become increasingly sophisticated, necessitating robust and adaptable defense mechanisms. Conventional risk discovery and examination strategies regularly drop brief in tending to energetic and determined assaults. Cyberattacks expanding complexity and recurrence require inventive devices and techniques to secure organized situations. To bridge this gap, virtualized environments like MetaRouter offer a controlled and replicable platform for studying cybersecurity threats and responses. By leveraging live forensic methods within such virtual lab networks, cybersecurity professionals can gain deeper insights into the behavior of threats and refine their strategies for mitigating them. Virtual labs provide a controlled setting for security professionals to analyze, detect, and mitigate threats effectively without risking production systems. Within the setting of improvement and testing, virtualization innovation can give disconnected situations, viably making virtual research facilities. This enables development teams to build and test applications without the need for additional physical infrastructure [3, 4]. One of the primary threats to such environments is network attacks, which can compromise data integrity, confidentiality, and availability. The Border Gateway Protocol (BGP) is utilized in the MetaRouter network to manage routing information exchange between routers. BGP is a routing protocol that exchanges routing information between autonomous systems (AS) on the internet or private networks. It is integral to internet infrastructure and is crucial in determining the best path for transmitting data between AS. BGP is commonly used by Internet Service Providers (ISPs) and large organizations to manage Internet traffic [5]. BGP's role in MetaRouter-based virtual networks highlights its importance in maintaining reliable and efficient communication across complex topologies. However, BGP is not without its vulnerabilities. Misconfigurations, route hijacking, and man-in-the-middle attacks are some of the threats that can exploit BGP's weaknesses. Analyzing these vulnerabilities within a virtual lab environment helps organizations develop robust strategies to secure their networks and enhance overall resilience. Live forensics is a critical aspect of modern cybersecurity investigations. Unlike traditional forensic methods, which rely on post-incident static data analysis, live forensics involves capturing volatile and dynamic information from running systems. This includes memory dumps, process activity, network traffic, and other ephemeral data that may disappear once the system is powered down. Live forensics is particularly valuable for analyzing ongoing attacks, providing real-time insights into attacker behavior and system vulnerabilities. By integrating live forensic methods into MetaRouter-based virtual networks, cybersecurity professionals can uncover hidden threats, analyze attack vectors, and devise effective countermeasures. This approach enhances security teams' detection and response capabilities and fosters a deeper understanding of the evolving threat landscape. Furthermore, virtual labs powered by MetaRouter offer unparalleled scalability and flexibility. Organizations can design and deploy complex network topologies. These studies' primary focus is improving security, identifying cyber threats, and creating replicable test environments. The following is a summary of the main studies, which can be seen in Table 1.

Table 1. State of The Art

Researcher(s)	Subject	Object of Study	Protocols	Data Collection	Data Analysis	Outcome
[6, 7]	Forensic Analysis on Routers	Routers	ICMP	Observations, Documentation	Data Validation	Enhanced attacker tracing methods and router security.
[8–10]	Enhancing Forensics on Servers	Servers	BGP, HTTP(S), TCP	Volatile & non-volatile data collection	AI-based anomaly detection	Scalable and automated forensic solutions for server security.
[7, 11]	Network Forensics Identification	Network Infrastructure	ICMP, ARP	Snort IDS, Packet Headers	Attack Lifecycle Analysis	Structured methodologies for network attack detection and documentation.
[12, 13]	Traffic Analysis in Virtual Routers	Virtual Routers	BGP, OSPF	Wireshark	Traffic Anomaly Detection	Insights into virtual routing dynamics and enhanced forensic methods.

Researcher(s)	Subject	Object of Study	Protocols	Data Collection	Data Analysis	Outcome
[14, 15]	ARP Protocol Forensics	ARP Protocol Behavior	ARP	Ettercap, ARP-Watch	Anomaly Detection Models	Improved detection and mitigation of ARP-based attacks.
[16–18]	Live Memory Analysis	Memory Snapshots	-	Memory Snapshot Tools	Volatile Data Analysis	Enhanced methods for leveraging live memory in forensics.
[12, 19, 20]	Machine Learning in Traffic Patterns	Network Traffic	ARP, BGP	Traffic Logs	ML Algorithms	Automated detection of network threats through traffic pattern recognition.
[21]	Cloud-Based Forensics	Cloud Environments	ICMP, TCP, ARP	Cloud-Native Tools	Scalable Analysis	Forensic scalability and efficiency in cloud platforms.
[12, 22, 23]	SDN Forensics	Software-Defined Networks	BGP, OSPF	Centralized Monitoring	Routing Path Analysis	Streamlined security approaches in SDN architecture.
[24, 25]	Hybrid Network Forensics	Physical & Virtual Routers	Mixed Protocols	Packet Captures (tcpdump)	Traffic Analysis	Comprehensive forensic strategies for hybrid network environments.

The difference between this study and previous studies is its focus on applying live forensic methodologies specifically designed for virtualized MetaRouter environments. While previous studies have emphasized forensic methodologies for physical routers [8–10], server environments [7, 11], and ARP-related attacks [16–18], this study uniquely integrates real-time traffic analysis and protocol-specific anomalies such as TCP port reuse, synchronize (SYN) session manipulation, and BGP hijacking. Unlike studies that use generic anomaly detection systems [21], this study uses Wireshark for live forensic data collection in a virtual lab environment designed to simulate realistic network traffic dynamics. Additionally, this study explores the interactions between routers and clients in a virtual environment, addressing unique challenges in virtualized network security that have not been explored in the existing literature. This study aims to improve the security and forensic capabilities of virtualized environments by identifying anomalies in routing behavior and packet data, primarily focusing on BGP anomalies and TCP-based irregularities. By leveraging tools such as Wireshark, this study aims to provide a replicable framework for detecting and documenting malicious activity, specifically in virtualized MetaRouter systems. This study contributes to the development of network forensics by advancing methodologies for live anomaly detection and real-time response in virtualized networks, which aligns with the broader goal of improving security in cloud-based and hybrid infrastructures. The contribution of this study are twofold. First, this study provides a practical framework for real-time forensic analysis in virtualized environments, bridging the gap between traditional forensic approaches and the needs of modern virtualized systems. Second, this study offers actionable insights for network administrators and cybersecurity professionals, including improved routing anomaly detection, enhanced BGP session stability, and robust defense mechanisms against potential hijacking attempts. By addressing the research gaps identified in studies [14, 15], and [12, 19, 20, 22, 23] this study paves the way for future advances in securing virtualized networks and hybrid cloud environments.

2. RESEARCH METHOD

Network forensic analysis in Virtual Computer Lab using Metarouter involves investigating digital footprints, log data, and network information to identify, analyze, and understand security incidents or suspicious activities. This study used action research, which is shown in Figure 1.

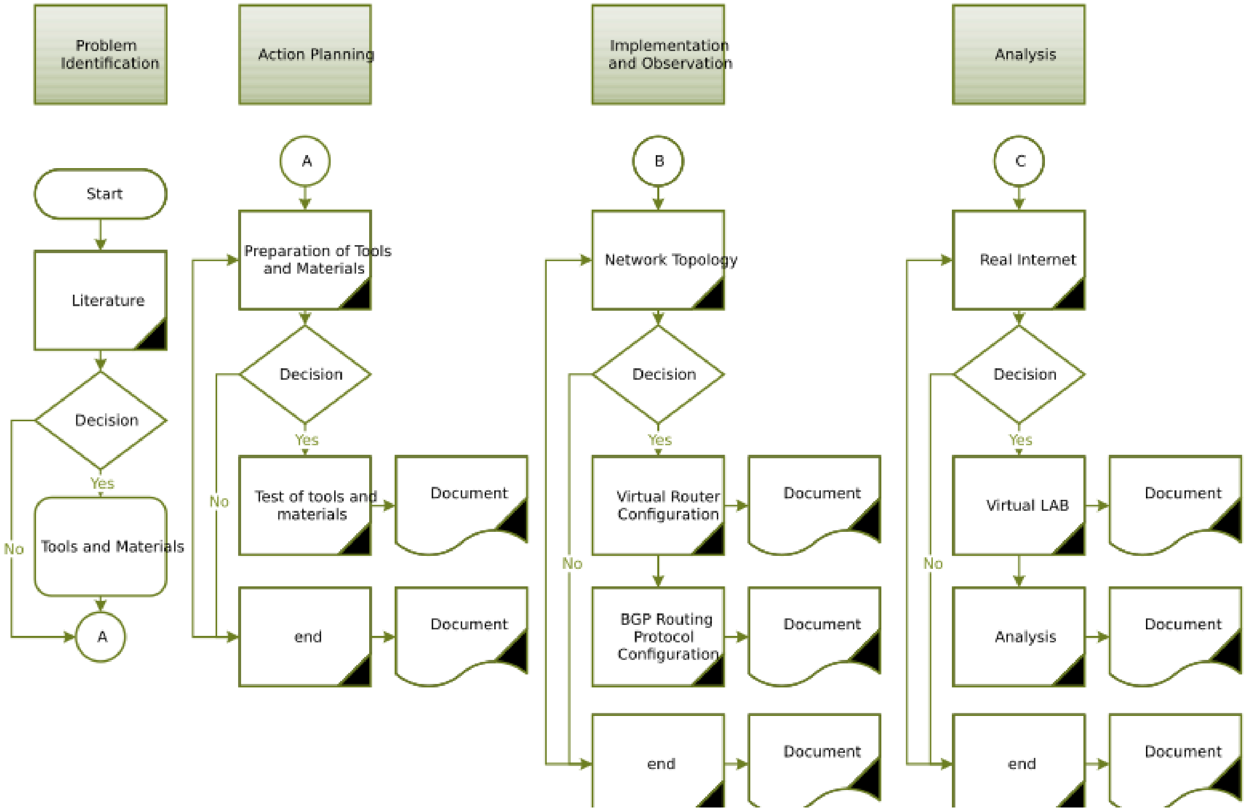


Figure 1. Research Flow

The problem identification stage is the initial stage of the research, namely by determining the problem or practical issue that needs to be addressed in a particular context by reviewing articles that lead to the title and results of previous research. The articles that have been collected will be discussed with the research team to determine what tools and materials will be used. The action planning stage is the stage of planning the actions to be implemented or the network infrastructure planning stage to address the identified problems, which includes preparing tools and materials and then conducting discussions to achieve research objectives. The discussion results will determine the tools and materials to be used, which will be tested before moving on to the next stage. Testing of tools and materials ends with a report and test documentation. The implementation and observation stages are the actions in carrying out the steps that have been set in the research flow and documenting the actions. It is important to discuss the network topology to be used in the research because this stage is the preparation stage of the forensic environment so that the next steps can be arranged neatly. Implementing a virtual router using Metarouter can be hampered if the network topology has not been determined. The same thing will happen to the BGP routing configuration. Each implementation step will be documented and reported at the final stage. The analysis stage is the final stage of the research conducted by the researcher, namely providing internet access to the virtual lab network that has been created. The research team discussion will be carried out regarding the forensic analysis that will be carried out on the virtual LAB computer network that has been built. The analysis stage involves determining the relevant data sources, including log files, network records, and memory snapshots. At the analysis stage, researchers will collect digital evidence related to the state of memory during the incident and network logs to look for signs of attack. Analysis of signs of an attack can be done by identifying suspicious activity in network log data. However, a network forensic tool is needed if this is unsuccessful in collecting evidence. All stages in the analysis stage will be documented and reported at the end of the analysis stage to obtain a complete report based on the established research flow. The diagram in the research action flow described in the study can be seen in Figure 2. The stages in the diagram encompass the entire process, from data collection to analysis, decision-making, and documentation, in the network forensic research conducted in a virtual laboratory using MetaRouter.

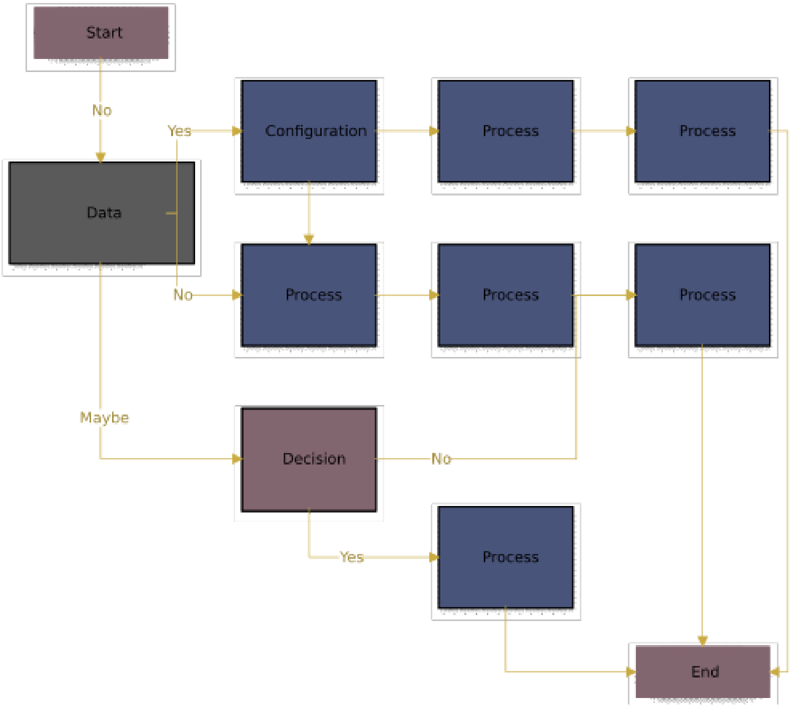


Figure 2. Action Research Flow

Figure 2 shows a flowchart that illustrates the process with several stages, decisions, and branching paths. Based on the research title description, this diagram represents the research flow of "Network Forensic Analysis in a Virtual Computer Lab Using MetaRouter," specifically the steps in action research. Start is the starting point of the research or investigation process. Data refers to the data collection or identification stage required for analysis, such as network logs, MetaRouter configuration, or memory snapshots. The decision represents the decision-making stage, where the collected data is evaluated to determine whether it is sufficient to proceed or if additional actions are required. Configuration involves configuring the network topology and implementing BGP on the MetaRouter to prepare the forensic environment. The process represents various stages in the research process, such as the implementation of the research steps, observation of network activities, collection of digital evidence, and analysis of log data and suspicious activities. The end is the final stage, summarizing the analysis and research findings, resulting in comprehensive documentation and a forensic report.

3. RESULT AND ANALYSIS

The findings clearly demonstrate that network anomalies, such as suspicious communication patterns, session manipulation, and route inconsistencies, are indicative of potential malicious activities. The results of this research are in line with previous research in the field of network security and attack detection. For example, the detection of TCP Port Reuse as a suspicious communication pattern is consistent with the findings of [6] and [7], which emphasizes the use of reused port numbers as an indicator of potential spoofing or unauthorized session activity. Similarly, the observation of SYN Floods and Session Manipulation, characterized by the transmission of SYN flags without a valid session completion, corroborates the findings in [18] where SYN floods were identified as a tactic to flood network resources or bypass security controls. The detection of Unauthorized Route Announcements, characterized by messages such as "Ignored Unknown Record" and sudden RST, ACK packets, supports previous studies such as [17], which highlights this anomaly as an important indicator of routing table manipulation and malicious route advertisements. Furthermore, this study identified Packet Data Anomalies, including "TCP Previous segment not captured" and "Out-Of-Order" packets, which were also documented in [24] and [25] as signs of disrupted traffic flow caused by potential packet injection or interception attacks. Lastly, the identification of BGP Hijacking Attempts in this study, evidenced by sudden RST packets, ACK anomalies, and Out-Of-Order patterns, is consistent with research by [12], which shows how such behavior often accompanies deliberate attempts to manipulate or hijack BGP sessions, leading to traffic redirection or denial of service. This comparison shows a strong correlation between the findings of this study and the existing literature, further validating the anomalies detected. Consistency with previous studies not only strengthens the credibility of this study but also highlights the need for continued refinement of detection and mitigation strategies for network threats in virtualized environments. The research results are summarized as shown in Table 2. Figure 3 simulates a network traffic attack involving communication between a web server, router, and client over the Internet.

Table 2. A Comparison of This Research's Findings

Anomaly/Threat	Current Research	Previous Studies
TCP Port Reuse	Detected suspicious communication patterns	[6, 7]
SYN Flood / Session Manipulation	SYN flags without valid session completions	[18]
Unauthorized Route Announcements	”Ignored Unknown Record” and RST, ACK messages	[17]
Packet Data Anomalies	”TCP Previous segment not captured” and ”Out-Of-Order”	[24, 25]
BGP Hijacking Attempts	Sudden RST, ACK packets, and Out-Of-Order patterns	[12]

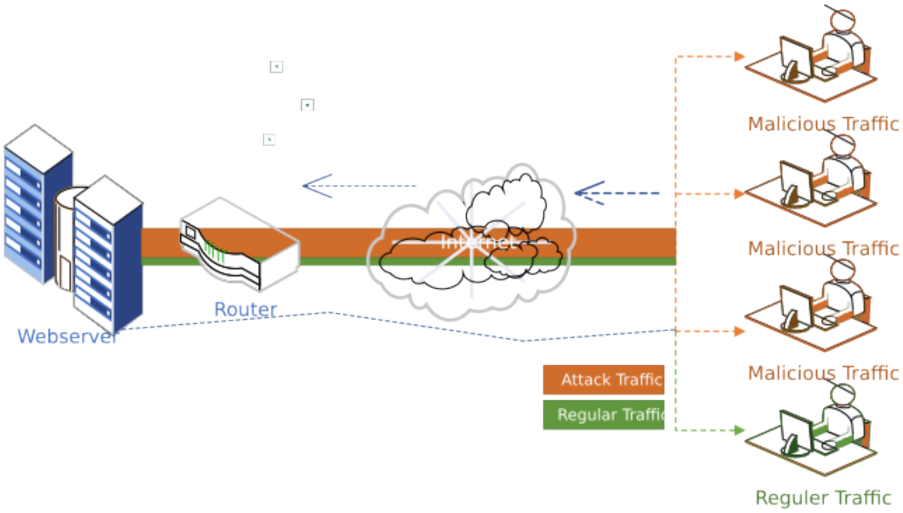


Figure 3. Simulation of a Prototype Network Malicious Traffic

Figure 3 is the diagram depicts a network traffic simulation involving communication between a web server, a router, and a client over the Internet. The web server acts as the source of data accessed by the client and is the primary target in both regular traffic and malicious attack scenarios. Routers connect web servers to the internet and manage data traffic, both incoming and outgoing. It is a critical point that is vulnerable to a variety of network attacks, including routing manipulation and protocol-based attacks. The Internet is the communication medium that connects the client to the server via the router and is the path through which regular and malicious traffic passes. On the right side, clients are categorized into two types: regular traffic, which is connected by the green line, and malicious traffic, which is connected by the orange line. Regular traffic is the normal activity of clients accessing the server for legitimate services without any malicious intent, while malicious traffic is traffic from attackers attempting to send malicious data, such as packet spoofing manipulation to disrupt the server or router. The colored arrows (green for regular traffic and orange for attack traffic) depict the interactions between the client, router, and web server. Malicious traffic attempts to exploit security vulnerabilities to compromise the system, while regular traffic is expected communication. This diagram depicts a simulation of a prototype network consisting of a web server, routers, and clients with normal and malicious traffic. The goal is to monitor these interactions, detect attack patterns such as spoofing or routing manipulation, and maintain the integrity of the system.

3.1. Configuration and Implementation

The MetaRouter was configured using Border Gateway Protocol (BGP) as the primary routing protocol to establish a dynamic network topology. This configuration aimed to create a virtual environment that closely mimics real-world network scenarios. The process began by defining the virtual network topology, ensuring efficient traffic management across interconnected nodes. Careful planning and setup were conducted to replicate the complexities of a modern network infrastructure. The network topology can be seen in Figure 4.

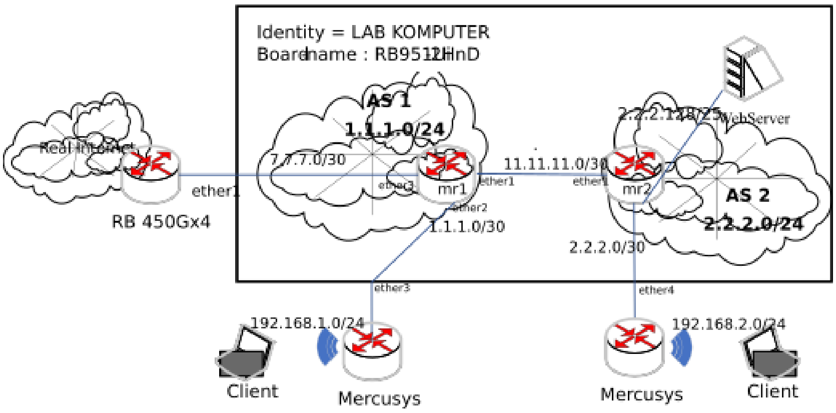


Figure 4. BGP Network Topology

Once the topology was defined, BGP routing was implemented to facilitate dynamic routing and simulate real-world network traffic patterns. This implementation allowed the network to adapt to changes in traffic flow and respond to routing updates dynamically. To ensure reliability, the MetaRouter configuration underwent rigorous testing to verify its stability and functionality. This testing phase ensured that the virtual environment was robust enough to handle simulated attacks and real-time forensic analysis. The results demonstrated that the configuration successfully established a functional and dynamic virtual network. The environment proved effective in capturing and logging data from simulated attacks, including unauthorized access attempts and BGP route manipulations. These logs provided valuable insights for further forensic analysis, showcasing the effectiveness of the setup in identifying and documenting network vulnerabilities.

3.2. Observation and Testing

The virtual lab environment was closely monitored during controlled experiments to identify potential vulnerabilities and evaluate the effectiveness of forensic tools. During these experiments, several suspicious activities were observed, including IP spoofing and unauthorized route announcements, indicating potential security breaches. Additionally, packet data anomalies were captured using Wireshark, revealing malicious payloads embedded within the network traffic. The experiments also highlighted the impact of these attacks on network performance, including disruptions to routing tables and overall network stability. As shown in Table 3, evidence of data access violations was uncovered.

Table 3. Summary of Captured Network Traffic

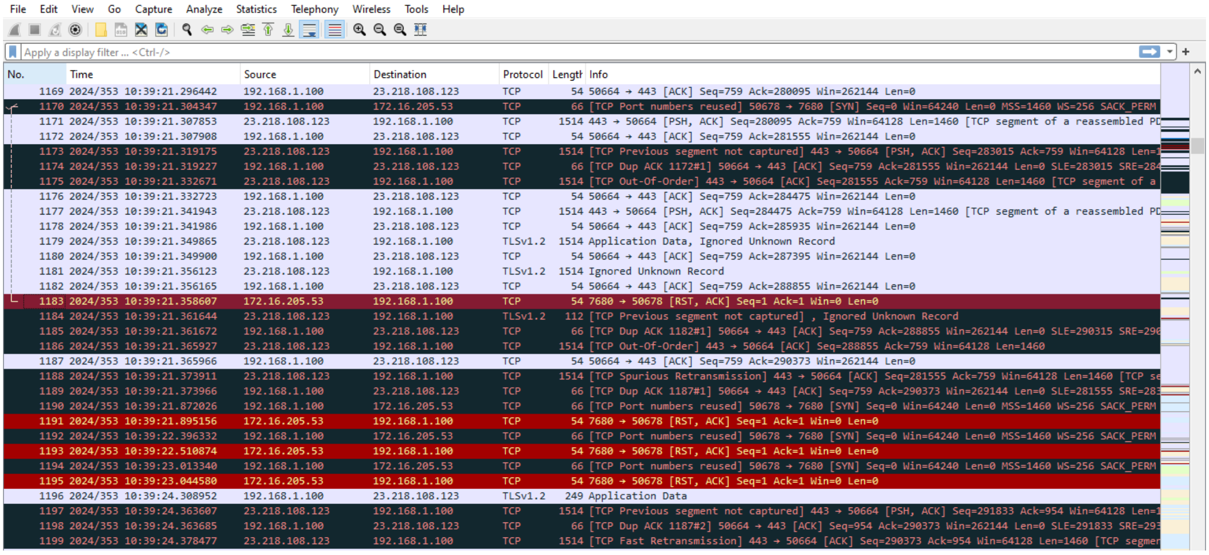
Normal	**Abnormal**
Length:	**Length:**
4385 kB	**1911 MB**
Format:	Format:
Wireshark/. . . - pcapng	Wireshark/... - pcapng
First packet:	**First packet:**
2024-12-18 10:32:52	**2024-12-18 12:44:51**
Last packet:	**Last packet:**
2024-12-18 12:33:39	**2024-12-18 14:45:00**
Elapsed:	**Elapsed:**
02:00:46	**02:00:08**

Normal	Abnormal
Hardware:	Hardware:
Intel(R) Core(TM) i5-3317U CPU @ 1.70GHz (with SSE4.2)	Intel(R) Core(TM) i5-3317U CPU @ 1.70GHz (with SSE4.2)
OS:	OS:
64-bit Windows 10 (22H2), build 19045	64-bit Windows 10 (22H2), build 19045
Application:	Application:
Dumpcap (Wireshark) 4.2.4 (v4.2.4-0-g1fe5bce8d665)	Dumpcap (Wireshark) 4.2.4 (v4.2.4-0-g1fe5bce8d665)
Statistics	Statistics
Measurement	Measurement
Captured	Captured
Displayed	Displayed
Marked	Marked
Packets	**Packets**
9085	**1295180**
9085 (100.0%)	**1295180 (100.0%)**
—	—
Average pps	**Average pps**
1.3	**179.7**
1.3	**179.7**
—	—
Average packet size, B	**Average packet size, B**
449	**1442**
449	**1442**
—	—
Bytes	**Bytes**
4079752	**1867224074**
4079752 (100.0%)	**1867224074 (100.0%)**
0	**0**
Average bytes/s	**Average bytes/s**
562	**259 k**
562	**259 k**
—	—
Average bits/s	**Average bits/s**
4503	**2072 k**
4503	**2072 k**
—	—

The captured file, measuring 1911 MB in size and saved in Wireshark's pcapng format, contains network traffic data collected over a period of 2 hours and 8 seconds (from 12:44:51 to 14:45:00 on December 18, 2024). The collection was performed using a system equipped with an Intel(R) Core (TM) i5-3317U CPU @ 1.70GHz and running a 64-bit version of Windows 10 (22H2). The Dumpcap utility from Wireshark version 4.2.4 was used to record the data. A total of 1,295,180 packets were captured and displayed in the analysis, with no packets marked or dropped. The average packet size recorded was 1,442 bytes, while the average packets per second (pps) rate was 179.7. The captured data totaled 1,867,224,074 bytes, equating to an average throughput of 259 kB/s or 2,072 kbit/s. The captured traffic exhibited abnormalities that indicated potential network intrusions or attacks. Examples include discrepancies in traffic patterns and packet anomalies, which suggest the possibility of malicious activities such as IP spoofing, unauthorized route announcements, or BGP hijacking attempts. These behaviors were identified through the analysis of packet data using tools such as Wireshark. The information gathered provides critical insights for further forensic investigation and response planning.

3.3. Analysis

The collected network data was meticulously analyzed to uncover attack patterns and identify potential vulnerabilities within the virtual lab environment. One of the most significant findings was evidence of Border Gateway Protocol (BGP) hijacking attempts. These incidents were characterized by unauthorized route injections, which disrupted the stability of the network and posed a serious security threat. Additionally, suspicious IP addresses involved in these activities were traced back to potential threat actors, aiding in the identification of malicious sources. The screenshot of Wireshark can be seen in Figure 5.



No.	Time	Source	Destination	Protocol	Length	Info
1169	2024/353 10:39:21.296442	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=280095 Win=262144 Len=0
1170	2024/353 10:39:21.304347	192.168.1.100	172.16.205.53	TCP	66	[TCP Port numbers reused] 50678 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1171	2024/353 10:39:21.307853	23.218.108.123	192.168.1.100	TCP	1514	443 → 50664 [PSH, ACK] Seq=280095 Ack=759 Win=64128 Len=1460 [TCP segment of a reassembled PD
1172	2024/353 10:39:21.307908	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=281555 Win=262144 Len=0
1173	2024/353 10:39:21.319175	23.218.108.123	192.168.1.100	TCP	1514	[TCP Previous segment not captured] 443 → 50664 [PSH, ACK] Seq=283015 Ack=759 Win=64128 Len=1
1174	2024/353 10:39:21.319227	192.168.1.100	23.218.108.123	TCP	66	[TCP Dup ACK 1172#1] 50664 → 443 [ACK] Seq=759 Ack=281555 Win=262144 Len=0 SLE=283015 SRE=284
1175	2024/353 10:39:21.332671	23.218.108.123	192.168.1.100	TCP	1514	[TCP Out-Of-Order] 443 → 50664 [ACK] Seq=281555 Ack=759 Win=64128 Len=1460 [TCP segment of a
1176	2024/353 10:39:21.332723	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=284475 Win=262144 Len=0
1177	2024/353 10:39:21.341943	23.218.108.123	192.168.1.100	TCP	1514	443 → 50664 [PSH, ACK] Seq=284475 Ack=759 Win=64128 Len=1460 [TCP segment of a reassembled PD
1178	2024/353 10:39:21.341986	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=285935 Win=262144 Len=0
1179	2024/353 10:39:21.349865	23.218.108.123	192.168.1.100	TLSv1.2	1514	Application Data, Ignored Unknown Record
1180	2024/353 10:39:21.349900	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=287395 Win=262144 Len=0
1181	2024/353 10:39:21.356123	23.218.108.123	192.168.1.100	TLSv1.2	1514	Ignored Unknown Record
1182	2024/353 10:39:21.356165	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=288855 Win=262144 Len=0
1183	2024/353 10:39:21.358607	172.16.205.53	192.168.1.100	TCP	54	7680 → 50678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1184	2024/353 10:39:21.361644	23.218.108.123	192.168.1.100	TLSv1.2	112	[TCP Previous segment not captured] , Ignored Unknown Record
1185	2024/353 10:39:21.361672	192.168.1.100	23.218.108.123	TCP	66	[TCP Dup ACK 1182#1] 50664 → 443 [ACK] Seq=759 Ack=288855 Win=262144 Len=0 SLE=290315 SRE=290
1186	2024/353 10:39:21.365927	23.218.108.123	192.168.1.100	TCP	1514	[TCP Out-Of-Order] 443 → 50664 [ACK] Seq=288855 Ack=759 Win=64128 Len=1460
1187	2024/353 10:39:21.365966	192.168.1.100	23.218.108.123	TCP	54	50664 → 443 [ACK] Seq=759 Ack=290373 Win=262144 Len=0
1188	2024/353 10:39:21.373911	23.218.108.123	192.168.1.100	TCP	1514	[TCP Spurious Retransmission] 443 → 50664 [ACK] Seq=281555 Ack=759 Win=64128 Len=1460 [TCP se
1189	2024/353 10:39:21.373966	192.168.1.100	23.218.108.123	TCP	66	[TCP Dup ACK 1187#1] 50664 → 443 [ACK] Seq=759 Ack=290373 Win=262144 Len=0 SLE=281555 SRE=283
1190	2024/353 10:39:21.872026	192.168.1.100	172.16.205.53	TCP	66	[TCP Port numbers reused] 50678 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1191	2024/353 10:39:21.895156	172.16.205.53	192.168.1.100	TCP	54	7680 → 50678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1192	2024/353 10:39:22.396332	192.168.1.100	172.16.205.53	TCP	66	[TCP Port numbers reused] 50678 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1193	2024/353 10:39:22.510874	172.16.205.53	192.168.1.100	TCP	54	7680 → 50678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1194	2024/353 10:39:23.013340	192.168.1.100	172.16.205.53	TCP	66	[TCP Port numbers reused] 50678 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1195	2024/353 10:39:23.044580	172.16.205.53	192.168.1.100	TCP	54	7680 → 50678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1196	2024/353 10:39:24.308952	192.168.1.100	23.218.108.123	TLSv1.2	249	Application Data
1197	2024/353 10:39:24.363607	23.218.108.123	192.168.1.100	TCP	1514	[TCP Previous segment not captured] 443 → 50664 [PSH, ACK] Seq=291833 Ack=954 Win=64128 Len=1
1198	2024/353 10:39:24.363685	192.168.1.100	23.218.108.123	TCP	66	[TCP Dup ACK 1187#2] 50664 → 443 [ACK] Seq=954 Ack=290373 Win=262144 Len=0 SLE=291833 SRE=293
1199	2024/353 10:39:24.378477	23.218.108.123	192.168.1.100	TCP	1514	[TCP Fast Retransmission] 443 → 50664 [ACK] Seq=290373 Ack=954 Win=64128 Len=1460 [TCP segmen

Figure 5. Screenshot of Wireshark

1. IP Spoofing

The captured data indicates suspicious communication between the IP addresses **192.168.1.100** and **172.16.205.53**. One notable observation is the presence of the message **"TCP Port numbers reused,"** which suggests that an old session has been reused for new communication. This behavior is often associated with spoofing or unauthorized activities. Additionally, there are patterns showing the transmission of packets with **SYN** flags without completing a valid session, indicating potential attempts at manipulating connections. These findings highlight abnormal activities in the network, possibly signaling malicious intent.

2. Unauthorized Route Announcements

The captured packets reveal indications of false routing information, as evidenced by messages such as **"Ignored Unknown Record"** and **"RST, ACK"** without any prior initiated communication. Furthermore, the IP address **192.168.1.100** is observed sending inconsistent responses, suggesting potential unauthorized route announcements. These anomalies indicate abnormal network behavior and possible malicious activity.

3. Packet Data Anomalies

The captured data indicates anomalies in packet transmission, as evidenced by messages such as **"TCP Previous segment not captured"** and **"TCP Out-Of-Order"**. These issues suggest potential disruptions in network traffic, including packet manipulation. Additionally, the message **"Spurious Retransmission"** highlights irregular packet retransmissions that do not align with the normal session sequence, further indicating abnormal network behavior.

4. BGP Hijacking Attempts

The indications of **"BGP route manipulation"** can be identified through patterns such as sudden **RST, ACK** packets that terminate a session abruptly. This often signifies attempts to disrupt legitimate BGP sessions and replace them with fraudulent routes. Furthermore, the combination of **RST, ACK** packets and packet anomalies, such as **Out-Of-Order**, strongly suggests deliberate efforts to manipulate routing paths within the network.

4. CONCLUSION

This research aimed to investigate the use of live forensic methods in virtual computer lab networks managed by MetaRouter, with a focus on identifying network threats such as unauthorized route announcements, packet manipulation, and BGP hijacking. The findings clearly demonstrate that network anomalies, such as suspicious communication patterns, session manipulation, and route inconsistencies, are indicative of potential malicious activities. By utilizing live forensic techniques, this research effectively captured and analyzed these network threats, providing valuable insights into their detection and mitigation. The novelty of this research lies in the application of live forensic methods to virtualized network environments, particularly in MetaRouter-managed networks, which are often overlooked in traditional forensics studies. This approach offers real-time monitoring and analysis capabilities, allowing for quicker detection of threats compared to traditional post-incident forensic analysis. The proposed method is particularly useful in identifying and responding to complex network attacks, such as BGP hijacking, that require rapid intervention. For further research, it is recommended to explore the integration of machine learning algorithms with live forensic methods to automate the detection of network anomalies. Additionally, expanding the scope to include other network management technologies beyond MetaRouter, such as Software-Defined Networking (SDN), could provide a broader understanding of virtualized network security. Future studies could also focus on developing advanced techniques for mitigating the identified threats in real-time, ensuring enhanced security and reliability in virtualized environments.

5. ACKNOWLEDGEMENTS

TThe authors would like to express their sincere gratitude to all individuals and organizations who contributed to the success of this research. Special thanks go to Universitas Islam Al-Azhar for providing the resources and support necessary to conduct this study. We are also grateful to the technical team for their invaluable assistance in setting up the virtual lab environment and ensuring the smooth execution of experiments. Additionally, we extend our appreciation to the developers of Wireshark and MetaRouter for their innovative tools, which were instrumental in the analysis and configuration processes. Finally, we acknowledge the guidance and constructive feedback from colleagues and mentors, which significantly improved the quality of this work.

REFERENCES

[1] F. Firmansyah and Y. H. Pratama, "Analisis Simulasi Mitigasi Ancaman ARP dan Round Trip Time pada Lalu Lintas DHCP VTP," *Progresif: Jurnal Ilmiah Komputer*, vol. 19, no. 1, p. 137, Feb. 8, 2023. DOI: 10.35889/progresif.v19i1.1086.

[2] S. Xiao, "VR Open Computer Network Virtual Laboratory Based on Big Data Technology," *Journal of Physics: Conference Series*, vol. 1648, no. 4, p. 042 105, Oct. 1, 2020. DOI: 10.1088/1742-6596/1648/4/042105.

[3] A. Luse and J. Rursch, "Using a virtual lab network testbed to facilitate real-world hands-on learning in a networking course," *British Journal of Educational Technology*, vol. 52, no. 3, pp. 1244–1261, May 2021. DOI: 10.1111/bjet.13070.

[4] B. Xie and S. M. Aghili, "McNeese Computer Networking Virtual Learning Environment," in *Advances in Information and Communication*, K. Arai, Ed., vol. 651, Cham: Springer Nature Switzerland, 2023, pp. 747–752. DOI: 10.1007/978-3-031-28076-4_53.

[5] J. Li, V. Giotsas, and S. Zhou, "Anatomy of Multipath BGP Deployment in a Large ISP Network," 2020. DOI: 10.48550/ARXIV.2012.07730.

[6] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *Jurnal Telekomunikasi dan Komputer*, vol. 10, no. 2, p. 111, Aug. 21, 2020. DOI: 10.22441/incomtech.v10i2.8757.

[7] H. A. Adjei *et al.*, "SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection)," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South): IEEE, Feb. 7, 2021, pp. 187–193. DOI: 10.23919/ICACT51234.2021.9370460.

[8] S. S. Vladimirov *et al.*, "Network Coding Datagram Protocol for TCP/IP Networks," *IEEE Access*, vol. 11, pp. 43 485–43 498, 2023. DOI: 10.1109/ACCESS.2023.3266289.

[9] Z. Bonok, "Sistem Informasi Berbasis Digital dengan Teknologi Virtual Office pada Laboratorium Teknik Elektro," *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, vol. 3, no. 2, pp. 168–174, Aug. 17, 2023. DOI: 10.51878/knowledge.v3i2.2412.

[10] D. Li, “Research on university laboratory network security based on Cloud Computing,” *Applied Mathematics and Nonlinear Sciences*, vol. 9, no. 1, p. 20 230 183, Jan. 1, 2024. DOI: 10.2478/amns.2023.1.00183.

[11] D. S. Sany, “Gamification Design of Computer Network Virtual Laboratory Using SAGD-VL Framework,” *MULTINETICS*, vol. 9, no. 1, pp. 1–12, Mar. 16, 2023. DOI: 10.32722/multinetics.v9i1.5165.

[12] A. Milolidakis *et al.*, “On the Effectiveness of BGP Hijackers That Evade Public Route Collectors,” *IEEE Access*, vol. 11, pp. 31 092–31 124, 2023. DOI: 10.1109/ACCESS.2023.3261128.

[13] B. F. Muhammad and I. C. Utomo, “Implementation of IDS Using Snort with Barnyard2 Visualization for Network Monitoring in The Informatics Engineering Computer Lab at Muhammadiyah University Surakarta,” *International Journal of Computer and Information System (IJCIS)*, vol. 4, no. 3, pp. 165–171, Dec. 26, 2023. DOI: 10.29040/ijcis.v4i4.142.

[14] C. Hao *et al.*, “Experiment Information System Based on an Online Virtual Laboratory,” *Future Internet*, vol. 13, no. 2, p. 27, Jan. 24, 2021. DOI: 10.3390/fi13020027.

[15] M. L. Santos and M. Prudente, “Effectiveness of Virtual Laboratories in Science Education: A Meta-Analysis,” *International Journal of Information and Education Technology*, vol. 12, no. 2, pp. 150–156, 2022. DOI: 10.18178/ijiet.2022.12.2.1598.

[16] E. Ariyanti, “Identifikasi Bukti Digital Instagram Web dengan Live Forensic pada Kasus Penipuan Online Shop,” *Cyber Security dan Forensik Digital*, vol. 4, no. 2, pp. 58–62, Apr. 19, 2022. DOI: 10.14421/csecurity.2021.4.2.2436.

[17] S. Bistarelli, A. Imparato, and F. Santini, “A TCP-based Covert Channel with Integrity Check and Retransmission,” in *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, Copenhagen, Denmark: IEEE, Aug. 21, 2023, pp. 1–7. DOI: 10.1109/PST58708.2023.10320204.

[18] M. F. Mohd Fuzi, N. F. Mohammad Ashraf, and M. N. F. Jamaluddin, “Integrated Network Monitoring using Zabbix with Push Notification via Telegram,” *Journal of Computing Research and Innovation*, vol. 7, no. 1, pp. 147–155, Mar. 30, 2022. DOI: 10.24191/jcrinn.v7i1.282.

[19] S. Manjunath *et al.*, “Machine Learning Techniques to Detect DDoS Attacks in IoT’s, SDN’s: A Comprehensive Overview,” *International Journal of Human Computations & Intelligence*, vol. 2, no. 4, pp. 203–211, Jun. 12, 2023. DOI: 10.5281/zenodo.8027034.

[20] F. Febriansyah, Z. Asti Dwiyanti, and Diash Firdaus, “Deteksi Serangan Low Rate DDoS pada Jaringan Tradisional Menggunakan Machine Learning dengan Algoritma Decision Tree,” *Cyber Security dan Forensik Digital*, vol. 6, no. 1, pp. 6–11, Aug. 16, 2023. DOI: 10.14421/csecurity.2023.6.1.3951.

[21] Y. B. Sanap and P. Aher, “A Comprehensive Survey On Detection And Mitigation Of DDoS Attacks Enabled With Deep Learning Techniques In Cloud Computing,” in *2023 6th International Conference on Advances in Science and Technology (ICAST)*, Mumbai, India: IEEE, Dec. 8, 2023, pp. 149–154. DOI: 10.1109/ICAST59062.2023.10454990.

[22] S. Amuda, M. F. Mulya, and F. I. Kurniadi, “Analisis dan Perancangan Simulasi Perbandingan Kinerja Jaringan Komputer Menggunakan Metode Protokol Routing Statis, Open Shortest Path First (OSPF) dan Border Gateway Protocol (BGP) (Studi Kasus Tanri Abeng University),” *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan)*, vol. 4, no. 2, pp. 53–63, Mar. 31, 2021. DOI: 10.47970/siskom-kb.v4i2.189.

[23] M. Revathi, V. V. Ramalingam, and B. Amutha, “A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework,” *Wireless Personal Communications*, vol. 127, no. 3, pp. 2417–2441, Dec. 2022. DOI: 10.1007/s11277-021-09071-1.

[24] P. Boyanov, “Investigating the Network Traffic Using the Command-Line Packets Sniffer Tcpdump in Kali Linux,” *Journal Scientific and Applied Research*, vol. 25, no. 1, pp. 31–44, Nov. 29, 2023. DOI: 10.46687/jsar.v25i1.378.

[25] P. Pangsuban, P. Nilsook, and P. Wannapiroon, “A Real-time Risk Assessment for Information System with CICIDS2017 Dataset Using Machine Learning,” *International Journal of Machine Learning and Computing*, vol. 10, no. 3, pp. 465–470, May 2020. DOI: 10.18178/ijmlc.2020.10.3.958.

[This page intentionally left blank.]