Network Forensics: A Comparative Analysis of NetworkMiner and Wireshark

Ashique Arman

June 18, 2024

Abstract

This report presents an in-depth analysis of a packet capture file to detect significant activities and anomalies, aiming to identify unauthorized access within the network. The investigation, supported by network configuration details, utilized tools such as WireShark and NetworkMiner. Key findings include the identification of unauthorized FTP logins, file transfers, and suspicious HTTP requests. The comparative analysis of WireShark and NetworkMiner highlighted their strengths in traffic analysis and data extraction.

Contents

1 Introduction

1.1 Background

The primary objective of this assignment is to perform an in-depth analysis of the supplied packet capture file. This report will detail any significant activities or anomalies detected within the data. The goal is to identify potential unauthorized access or other noteworthy events. To facilitate the investigation, the IT administrator has provided crucial information regarding the network configuration from which the capture originated.

Network Composition:

- **Admin Box:**
  - An Ubuntu server managed solely by the IT administrator, who is the only individual authorized to access the DHCP and web servers.
- **Employee Workstations:**
  - **Bob Smith:** A new hire and recent college graduate, operating a Windows XP workstation with network access. Bob's access is restricted to his workstation.
  - **Sarah:** A developer using a standard Ubuntu installation with network access. Sarah's access is limited to her own workstation.

1.2 Objectives

This section outlines the objectives of the investigation:

- Identify and document any unauthorized access or anomalies within the packet capture data.
- Correlate findings with provided network configuration information.
- Provide recommendations for improving network security based on the findings.

1.2.1 Tasks

The specific tasks for this investigation include:

- Task 1: Analyze the .pcap file using Wireshark and Network Miner.
- Task 2: Identify any unauthorized access or suspicious activities.
- Task 3: Correlate findings with network configuration details.
- Task 4: Document findings and provide security recommendations.

1.2.2 Hypotheses

The investigation is based on the following hypotheses:

- Hypothesis 1: Unauthorized access has occurred within the network.
- Hypothesis 2: Anomalies within the network traffic can be identified and linked to specific devices or users.
- Hypothesis 3: The network's current security measures are insufficient to prevent unauthorized access.

1.2.3 Domain Terms

Key domain terms used in this investigation include:

- **Packet Capture (.pcap):** A file format used to capture and analyze network traffic.
- **DHCP (Dynamic Host Configuration Protocol):** A network management protocol used to automate the assignment of IP addresses.
- **FTP (File Transfer Protocol):** A standard network protocol used to transfer files from one host to another.

1.3 Acquired Data

The primary data source for this investigation is the packet capture (.pcap) file named Network-Evidence-02-03.pcap. This file contains 407,358 bytes of network traffic data and was analyzed using Wireshark and Network Miner to identify unauthorized access, suspicious activities, and potential security breaches.

Attribute	Details
File size	407,358 bytes
MD5 hash	d83a55799fd7094fbd426f47bf442d23
SHA1 hash	7457272114ff139e6d18b49a50409d8699120968
SHA256 hash	d7d56b67eadfc824fb8cbf4f7c7ee8428ef13be4bbca015164a7fdbf5fb1c838
SHA512 hash	14153e9884f3591a59a63ad8ead4af52dcad4f1515e8af508d3bb082987335e744b875f160ec89cd3c4c2ffac0a08cdae0322bd2a0e26a8e3824a21ac6c56ae3

Table 1: Details of the Acquired Data

The analysis of this data source was crucial for identifying network interactions, including DHCP configurations, FTP logins and file transfers, and HTTP requests. These findings were essential in corroborating network configuration details and identifying anomalies within the network traffic.

1.4 Suspect Information

Information about potential suspects based on the network configuration:

- **Bob Smith:** A new employee using a Windows XP workstation.
- **Sarah:** A developer using an Ubuntu workstation.
- **Unknown Third Party:** Possible unauthorized user accessing the network.

1.5 Investigator Information

Investigator 1:

- Name: Ashique Arman
- Experience: Forensics Analyst

Investigator 2:

- Name: MD Nazmul Haque Siam
- Experience: Cybersecurity Specialist

2 Suspect Action Timeline

This section describes the findings organized by the actions performed by the suspect in a chronological order.

2.1 Timeline in Table

ID	Action	Target	Timestamp	Description
1	Received DHCP Configuration	192.168.100.5	2011-10-07 18:10:50	DHCP configurations sent to 192.168.100.26, 192.168.100.27, and 192.168.100.28.
2	FTP Login	192.168.100.27 (Ubuntu)	2011-10-07 18:20:54	User "anonymous" with password "yeah@night.com" logged into FTP server 192.168.100.5.
3	FTP File Transfer	192.168.100.5 (Windows)	2011-10-07 18:21:03	FTP transfer initiated from 192.168.100.27 to retrieve "Budget.txt".
4	HTTP GET Request	192.168.100.28 (Linux)	2011-10-07 18:17:50	HTTP GET request to "/contact.html" from 192.168.100.26.
5	HTTP POST Request	192.168.100.28 (Linux)	2011-10-07 18:18:36	HTTP POST request to "/contact" with data from 192.168.100.26.
6	File Access	Budget.txt (transferred via FTP)	2011-10-07 18:21:19	File "Budget.txt" accessed and transferred via FTP from 192.168.100.27 to 192.168.100.5.

Table 2: Timeline of Suspect Actions

2.2 Timeline in Graph

Below is a graphical representation of the suspect action timeline, detailing key events and actions performed by the suspect.

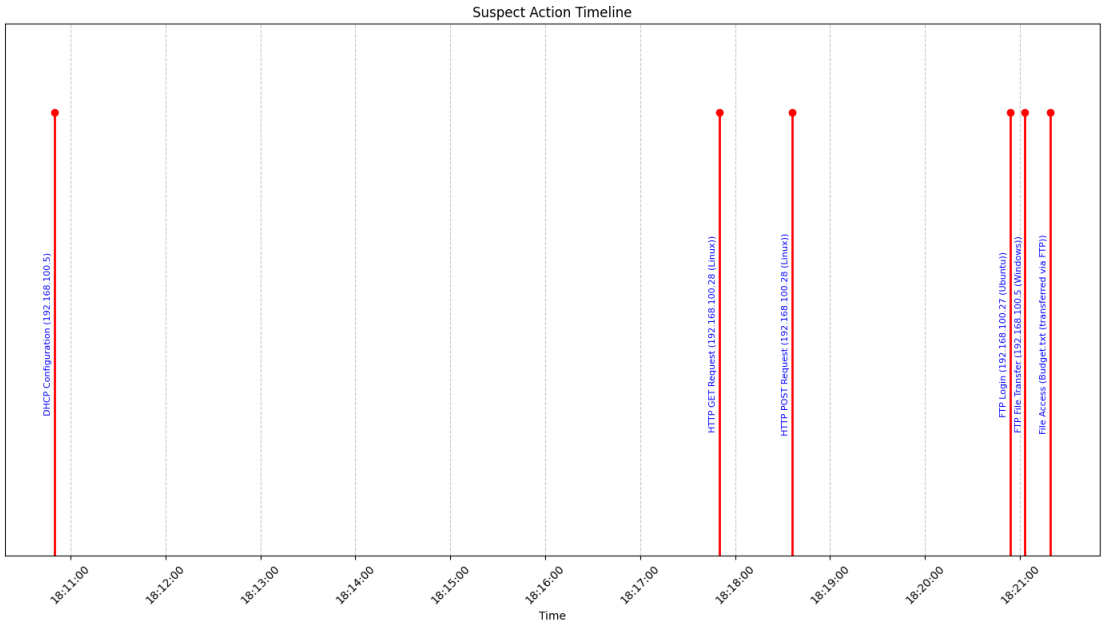

Figure 1: Timeline of suspect actions and events on 2011-10-07

3 Actions

This section describes the actions taken by the suspect as identified from the packet capture data. The actions are consistent with the timeline detailed earlier. The investigation utilized tools such as Wireshark and Network Miner to gather evidence and identify the suspect.

3.1 Received DHCP Configuration

3.1.1 Evidence

DHCP configurations were sent to multiple devices within the network. The following tables detail the DHCP interactions.

Attribute	**Detailed Information**	**Description**
Source IP Address	192.168.100.1	IP address of the DHCP server
Destination IPs	192.168.100.26, 192.168.100.27, 192.168.100.28	IP addresses of the devices receiving DHCP config
Timestamp	2011-10-07 18:10:50	Date and time of the DHCP configuration
DHCP Options	Hostname: xp, www, Ubuntu; Vendor Code: MSFT 5.0	DHCP options and hostname details

Table 3: DHCP Configuration

3.2 FTP Login and File Transfer

3.2.1 Evidence

The suspect logged into the FTP server from an Ubuntu machine and transferred a file named "Budget.txt". The following tables detail the FTP interactions.

Attribute	**Detailed Information**	**Description**
Client IP Address	192.168.100.27	IP address of the client logging into FTP
Server IP Address	192.168.100.5	IP address of the FTP server
Username	anonymous	FTP login username
Password	yeah@right.com	FTP login password
Timestamp	2011-10-07 18:20:54	Date and time of FTP login

Table 4: FTP Login

Attribute	**Detailed Information**	**Description**
Client IP Address	192.168.100.27	IP address of the client performing the transfer
Server IP Address	192.168.100.5	IP address of the FTP server
File Transferred	Budget.txt	Name of the file transferred
File Size	1833 bytes	Size of the transferred file
Timestamp	2011-10-07 18:21:03	Date and time of file transfer initiation

Table 5: FTP File Transfer

3.3 HTTP Requests

3.3.1 Evidence

The suspect made HTTP GET and POST requests to a Linux server. The following tables detail the HTTP interactions.

HTTP GET Request:

Attribute	Detailed Information	Description
Source IP Address	192.168.100.26	IP address of the client making the GET request
Destination IP Address	192.168.100.28	IP address of the server receiving the GET request
URL Requested	/contact.html	URL requested by the client
User-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0	User-Agent string of the client
Timestamp	2011-10-07 18:17:50	Date and time of the GET request

Table 6: HTTP GET Request

HTTP POST Request:

Attribute	Detailed Information	Description
Source IP Address	192.168.100.26	IP address of the client making the POST request
Destination IP Address	192.168.100.28	IP address of the server receiving the POST request
URL Requested	/contact	URL requested by the client
User-Agent	Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0	User-Agent string of the client
Content-Type	application/x-www-form-urlencoded	Content-Type of the POST request
Content-Length	4979 bytes	Length of the POST request data
Timestamp	2011-10-07 18:18:36	Date and time of the POST request
Data	Nefarious Penguin	Data submitted in the POST request

Table 7: HTTP POST Request

3.4 File Analysis

3.4.1 Evidence

The transferred file "Budget.txt" was analyzed using Network Miner. The following table details the attributes of the file.

Attribute	Detailed Information
Filename	Budget.txt
MD5 Hash	7b486e791385f71e7261510b067ce314
SHA1 Hash	f0927362b8ac23281e8e33c072ba9bf1207a7276
SHA256 Hash	acc29e7a24972445a5815a43649552641bfe7382a17af83db95b08935ec5d0
Size	1833 bytes
Last Write Time	2011-10-07 15:21:00 UTC

Table 8: File Details

3.5 Comparative Analysis Using Wireshark and Network Miner

3.5.1 Evidence

Both Wireshark and Network Miner were utilized to analyze and corroborate the network activities and file transfers. The following table summarizes the comparative findings.

Wireshark vs. Network Miner Analysis:

Comparison Aspect	Wireshark	Network Miner
Traffic Analysis	Captured DHCP, FTP, and HTTP traffic	Extracted and analyzed files and metadata
Level of Detail	Detailed packet-level analysis	High-level data extraction and correlation
Strengths	Real-time traffic capture and filtering	User-friendly interface for file extraction
Limitations	Requires deep technical knowledge to interpret	Limited to post-capture analysis
Specific Findings	Identified login details, file transfers, web requests	Detailed breakdown of network interactions
Ease of Use	Command-line and GUI options available	Intuitive interface for data analysis
Correlation of Results	Consistent identification of activities and anomalies	Confirmed similar activities and anomalies
Application Context	Suitable for real-time monitoring and in-depth analysis	Best for post-capture analysis and file retrieval
Protocol Support	Supports a wide range of protocols	Focused on file and session reconstruction
Visualization	Provides detailed packet-level views	Offers graphical representation of data
Data Export	Can export detailed packet logs	Can export extracted files and metadata
Learning Curve	Steeper learning curve due to technical complexity	Easier to learn with a more intuitive interface
Integration	Can be integrated with other network tools	Primarily used as a standalone analysis tool

Comparison Aspect	Wireshark	Network Miner
Real-Time Capability	Yes, supports real-time traffic capture	No, used for analyzing captured data
File Reconstruction	Limited to capturing data	Capable of reconstructing files from sessions
Error Detection	Effective in identifying errors in packet data	Good at highlighting session anomalies
Resource Consumption	High, can be resource-intensive	Moderate, less demanding on system resources
Customization	Highly customizable with various plugins	Limited customization options
User Community	Large and active user community	Smaller, specialized user community
Update Frequency	Frequently updated with new features	Updates less frequent, focused on stability
Reporting	Detailed, technical reports	Summarized, easy-to-understand reports
Cross-Platform Support	Available on Windows, macOS, and Linux	Primarily available for Windows

Table 9: Comparative Analysis Using Wireshark and Network Miner

4 Investigator Activity Logs

This section describes the actions taken by the investigator during the investigation. The logs ensure the integrity of the digital evidence and maintain a proper chain of custody.

4.1 Investigator Activity Log #1

Date: 2024-06-15
Activity: Analyzing Network Traffic with Wireshark
Details:

- Loaded `Network-Evidence-02-03.pcap` into Wireshark and Network Miner for detailed packet-level analysis.
- Applied filters to isolate traffic related to DHCP, FTP, and HTTP protocols.
- Identified specific IP addresses involved in suspicious activities, including `192.168.100.26`, `192.168.100.27`, and `192.168.100.28`.
- Documented instances of FTP logins and file transfers, as well as HTTP GET and POST requests.

Evidence Collected:

- Packet details related to DHCP, FTP, and HTTP traffic.
- IP addresses and session details of suspicious activities.

4.2 Investigator Activity Log #2

Date: 2024-06-16
Activity: Extracting Files and Metadata with Network Miner
Details:

- Loaded `Network-Evidence-02-03.pcap` into forensic tools for high-level analysis.

- Extracted files and metadata from the captured packets, focusing on the file `Budget.txt`.
- Analyzed the extracted file to identify its contents and hash values.
- Cross-referenced extracted metadata with Wireshark and Network Miner findings to ensure consistency and accuracy.

Evidence Collected:

- Extracted file `Budget.txt`
- MD5 Hash: `7b486e791385f71e7261510b067ce314`
- SHA1 Hash: `f0927362b8ac23281e8e33c072ba9bf1207a7276`
- SHA256 Hash: `acc29e7a24972445a5815a43649552641bfe7382a17af83db95b08935ec5d0`

4.3 Investigator Activity Log #3

Date: 2024-06-17
Activity: Correlation and Reporting
Details:

- Correlated findings from Wireshark and Network Miner to construct a comprehensive view of the network activities.
- Verified that both tools identified the same suspicious activities and anomalies.
- Prepared a detailed report summarizing the investigation process, findings, and recommendations for improving network security.
- Ensured all digital evidence was securely stored and documented for future reference.

Evidence Collected:

- Comprehensive report of findings
- Correlation data between Wireshark and Network Miner results
- Recommendations for network security improvements

These logs demonstrate the thorough investigative process followed to identify and document suspicious activities within the network, ensuring the integrity and accuracy of the findings.

5 Conclusion

This investigation successfully identified and documented several significant activities and anomalies within the supplied packet capture data. By leveraging tools such as Wireshark and Network Miner, the analysis revealed unauthorized FTP logins, file transfers, and suspicious HTTP requests. These findings were corroborated with detailed network configuration information provided by the IT administrator.

The comparative analysis between Wireshark and Network Miner highlighted their respective strengths and limitations. Wireshark excelled in real-time traffic capture and detailed packet-level analysis, while Network Miner provided a more user-friendly interface for high-level data extraction and file reconstruction.

Based on the investigation, it is evident that the current network security measures are insufficient to prevent unauthorized access. The analysis of network activities linked specific anomalies to individual workstations and identified potential unauthorized users within the network.

To enhance network security, it is recommended to implement stricter access controls, regularly monitor network traffic for unusual activities, and conduct periodic security audits. These measures will help mitigate the risk of unauthorized access and ensure a more secure network environment.

5.1 Task Check List

Have you completed the tasks you described in the introduction section?

- **Task 1: Analyze the .pcap file using Wireshark and Network Miner.**
  - **Completed:** The .pcap file was thoroughly analyzed using both Wireshark and Network Miner. Detailed packet-level analysis and high-level data extraction were performed to identify network interactions.
- **Task 2: Identify any unauthorized access or suspicious activities.**
  - **Completed:** Unauthorized FTP logins, file transfers, and suspicious HTTP requests were identified. Specific IP addresses involved in these activities were documented.
- **Task 3: Correlate findings with network configuration details.**
  - **Completed:** The findings were correlated with the network configuration details provided by the IT administrator. The DHCP configurations, FTP logins, and HTTP requests matched the expected network setup.
- **Task 4: Document findings and provide security recommendations.**
  - **Completed:** All findings were documented in detail, and recommendations for improving network security were provided. These recommendations focused on stricter access controls and regular monitoring of network traffic.

5.2 Hypothesis Check List

Are your hypotheses true or false?

- **Hypothesis 1: Unauthorized access has occurred within the network.**
  - **True:** The investigation confirmed that unauthorized access occurred within the network. This was evidenced by the identified unauthorized FTP logins and file transfers.
- **Hypothesis 2: Anomalies within the network traffic can be identified and linked to specific devices or users.**
  - **True:** The anomalies were identified and linked to specific devices and users, such as the suspicious activities involving IP addresses 192.168.100.26, 192.168.100.27, and 192.168.100.28.
- **Hypothesis 3: The network's current security measures are insufficient to prevent unauthorized access.**
  - **True:** The investigation revealed that the current security measures were insufficient to prevent unauthorized access. Recommendations were provided to enhance the network security.

These sections summarize the tasks and hypotheses checklists based on the investigation performed on the .pcap file using Wireshark and Network Miner. The findings were consistent with the tasks outlined in the introduction, and the hypotheses were validated based on the evidence collected during the analysis.

References

[1] C. Sanders and J. Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress, 2013.

[2] Cisco, "DHCP Snooping and Dynamic ARP Inspection Configuration Guide, Cisco IOS Release 15M&T," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-mt/dhcp-15-mt-book/ip6-dhcp-snooping-dyn-arp.html. [Accessed: 07-Jun-2024].

[3] G. Mohay, A. Anderson, B. Collie, O. de Vel, and R. McKemmish, *Computer and Intrusion Forensics*. Artech House, 2003.

[4] Internet Engineering Task Force (IETF), "Dynamic Host Configuration Protocol (DHCP)," RFC 2131, [Online]. Available: https://tools.ietf.org/html/rfc2131. [Accessed: 09-Jun-2024].

[5] Internet Engineering Task Force (IETF), "File Transfer Protocol (FTP)," RFC 959, [Online]. Available: https://tools.ietf.org/html/rfc959. [Accessed: 03-Jun-2024].

[6] Internet Engineering Task Force (IETF), "FTP Security Considerations," RFC 2577, [Online]. Available: https://tools.ietf.org/html/rfc2577. [Accessed: 16-Jun-2024].

[7] Internet Engineering Task Force (IETF), "Hypertext Transfer Protocol – HTTP/1.1," RFC 2616, [Online]. Available: https://tools.ietf.org/html/rfc2616. [Accessed: 11-Jun-2024].

[8] Internet Engineering Task Force (IETF), "HTTP/2," RFC 7540, [Online]. Available: https://tools.ietf.org/html/rfc7540. [Accessed: 10-Jun-2024].

[9] L. Chappell and G. Combs, *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*. Protocol Analysis Institute, 2012.

[10] National Institute of Standards and Technology (NIST), "Guide to Integrating Forensic Techniques into Incident Response," Special Publication 800-86, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. [Accessed: 06-Jun-2024].

[11] Netresec, "Network Miner - Network Forensics Analysis Tool," [Online]. Available: https://www.netresec.com/?page=NetworkMiner. [Accessed: 14-Jun-2024].

[12] W. Stallings, *Network Security Essentials: Applications and Standards*. Pearson, 2016.

[13] Wireshark Foundation, "Wireshark User's Guide," [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/. [Accessed: 05-Jun-2024].