PCAP FILE ANALYSIS USING WIRESHARK

Minor-2 Project Report

Salvam Kanna | Semester: 3rd

Subject: Cyber Security / Network Security

Project Title: Analysis of Network Traffic Using PCAP

PROJECT FOUNDATION

Introduction and core objectives of the cybersecurity investigation.

1. INTRODUCTION

- **Cybersecurity Monitoring:** Crucial field in computer engineering where network traffic is analyzed to detect malicious activities.
- **PCAP Data:** Contains network communication data used to analyze attacks and identify suspicious behavior.
- **Analytical Goal:** Understand how attackers operate and identify system vulnerabilities through packet forensics.
- **Context:** This project focuses on identifying an attacker and victim, detecting port scans, and retrieving hidden data.

2. PROJECT OBJECTIVES

ANALYSIS

Master the use of Wireshark for deep PCAP file examination.

IDENTIFICATION

Distinguish between Attacker and Victim IP addresses accurately.

EXTRACTION

Learn to isolate and extract files from live HTTP network traffic.

CAPTURE

Successfully retrieve the hidden flag from the extracted ZIP file.

3. TOOLS USED

Tool	Functional Description
Wireshark	Advanced network packet analyzer for deep packet inspection.
Windows OS	Main system environment utilized for the analysis process.
ZIP Extractor	Utility used to unzip downloaded artifacts from traffic.
Google Docs	Documentation platform used for reporting findings.

4. METHODOLOGY

The **ctf.pcapng** file was loaded into Wireshark for multi-stage analysis:

- Applied display filters (TCP, HTTP) to isolate relevant traffic.
- Analyzed TCP SYN packets to identify reconnaissance patterns.
- Utilized Conversation Details for flow mapping.
- Used **HTTP Export Objects** to carve out file artifacts.

5. ACTOR IDENTIFICATION

ATTACKER IP: 192.168.29.10

- Initiated multiple **TCP SYN** packets.
- Scanned high volumes of victim ports.
- Hosted malicious ZIP file on an HTTP server.

VICTIM IP: 192.168.29.155

- Target of intensive port scanning activity.
- Received suspicious HTTP file requests.
- Operates within the local private IP range.

5.3 FIRST PACKET TIMESTAMP

0.0000

Seconds

INITIAL CONTACT

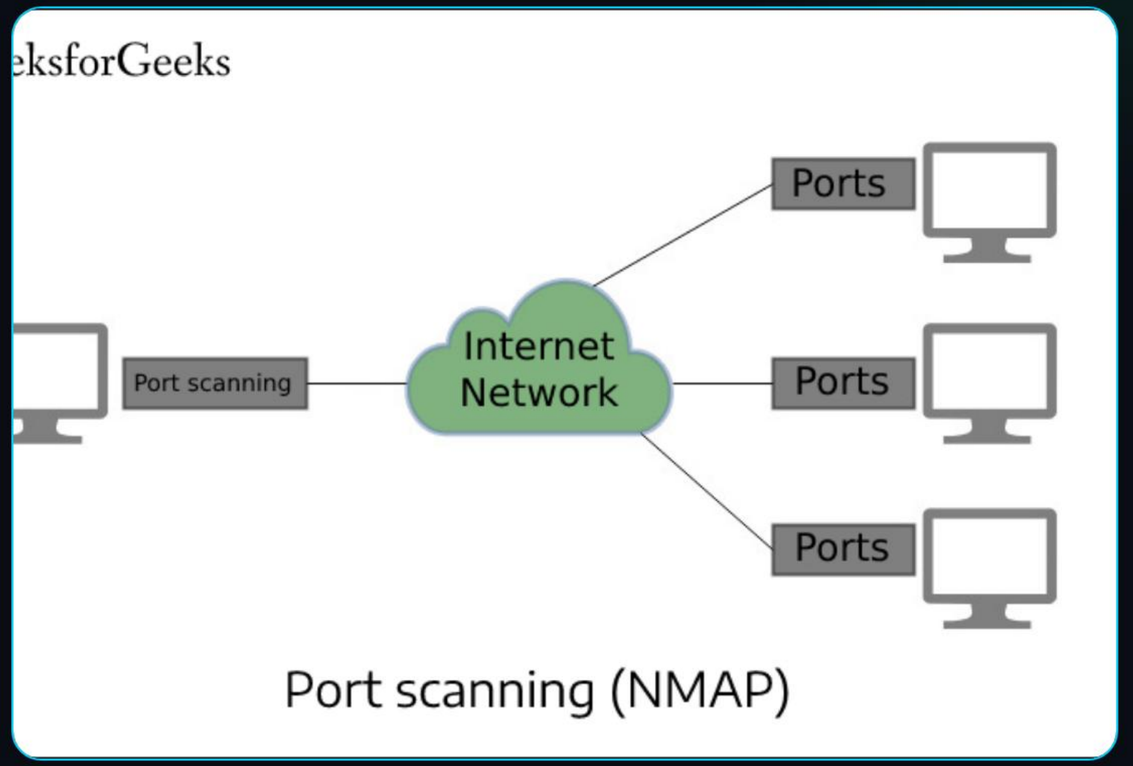
The first suspicious packet was recorded at exactly 0.000000000 seconds. This timestamp marks the precise start of the reconnaissance phase where the attacker began probing the target network environment.

5.4 EVIDENCE OF PORT SCANNING

The reconnaissance phase was confirmed using the following filter:

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

- Observed multiple SYN packets in rapid succession.
- Sequences targeted different destination ports.
- Consistent Source-Destination IP pairs indicated automated scanning scripts.



5.5 HTTP DATA EXTRACTION

Analysis of HTTP traffic (filter: `http`) revealed a GET request for a suspicious archive:

```
GET /dog_flag.jpg.zip HTTP/1.1
```

Using Wireshark's "Export Objects" feature, the **dog_flag.jpg.zip** file was successfully carved from the TCP stream, confirming successful data exfiltration from the attacker's server.

6. THE CAPTURED FLAG

After extraction and unzipping, the image **dog_flag.jpg** was analyzed.

PKHUYR{DOGESH_BHAI_JINDABAD}

Mission Accomplished: Flag Successfully Retrieved.

CONCLUSION

This project demonstrated the practical application of network traffic analysis. By identifying attacker patterns and extracting hidden data, we gained deeper insights into cybersecurity forensics.

THANK YOU!

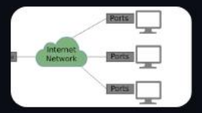
Guided by: **Prashant Sir**

Presented by: **Salvam Kanna**

IMAGE SOURCES

https://upload.wikimedia.org/wikipedia/commons/thumb/d/df/Wireshark_icon.svg/2048px-Wireshark_icon.svg.png

Source: commons.wikimedia.org



https://media.geeksforgeeks.org/wp-content/uploads/20220520112919/portscanning.jpg

Source: www.geeksforgeeks.org

https://media.istockphoto.com/id/1411195925/photo/exchange-information-and-data-with-internet-cloud-technology-ftp-files-receiver-and-computer.jpg?s=612×612&w=0&k=20&c=_XiI_tL4dpzKJlDLXQNFi0QcQfCFOgb99B71c-GD4T0=

Source: www.istockphoto.com

https://elements-resized.envatousercontent.com/elements-video-cover-images/67a18946-2d32-44b5-978c-406b8fb84184/video_preview/video_preview_0000.jpg?w=500&cf_fit=cover&q=85&format=auto&s=24d0629c8f2b4dba33174cf90f537e02f0a9f8ccba06f2fa1b4bc2419e9f0c84

Source: elements.envato.com