Cybersecurity Research Paper: Threat Analysis and Network Packet Investigation Using Wireshark

Abstract:

This research project focuses on studying critical cybersecurity threats and applying practical network traffic analysis techniques using Wireshark. The aim is to develop an understanding of common cyberattacks and practice detecting them through real-world network packet captures (.pcap files).

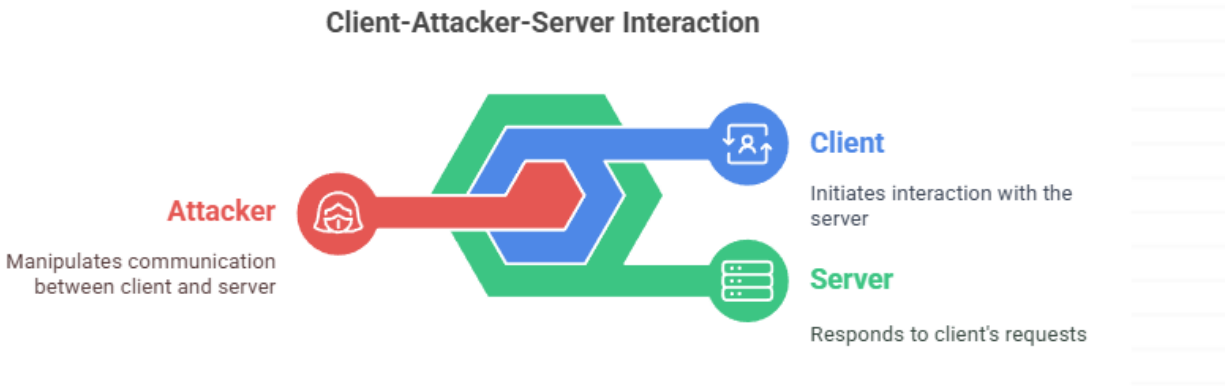
Table of Contents

Introduction

This report provides an overview of common cyber threats and associated control measures, as well as a practical network analysis using the Wireshark tool. The aim is to demonstrate technical skill and theoretical knowledge necessary for a job as a Cybersecurity Operations Analyst.

PART A: Research Report – Common Cyber Attacks & Controls

1. Man-in-the-Middle (MITM) Attack



1. Man-in-the-Middle (MITM) Attack

A Man-in-the-Middle (MITM) attack is where an attacker silently intercepts, observes, or alters communication between two parties without their knowledge. Victims believe they are communicating directly with each other, but in reality, the attacker is in the middle, intercepting and potentially altering the information being communicated. MITM attacks can be launched against email communication, web sessions, or open Wi-Fi networks. Session hijacking, DNS spoofing, ARP poisoning, and SSL stripping are popular techniques. These attacks are also highly dangerous since users will not notice any sign of interception.

Control Mechanisms:

To avoid MITM attacks, organizations must enforce the usage of strong encryption protocols such as HTTPS and TLS/SSL across all communication channels. Virtual Private Networks (VPNs) also provide an additional layer of encryption, especially when personnel access public networks. Public key infrastructure (PKI) certificates must be authenticated for legitimacy. Additionally, implementing secure Wi-Fi authentication protocols such as WPA3, and enforcing network segmentation can also limit exposure to MITM vulnerabilities. Example: Public Wi-Fi hotspots that are not encrypted are notorious for enabling MITM attacks on unsuspecting customers (Rouse, 2020).

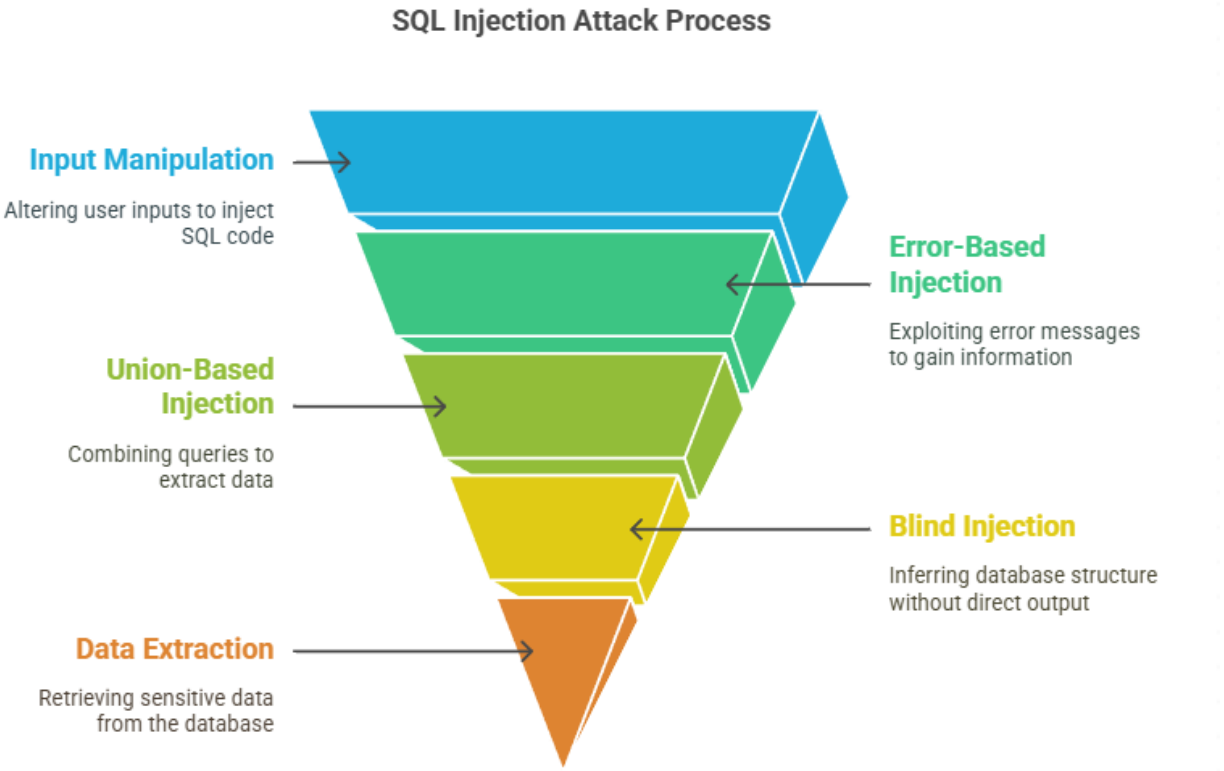
2. Denial-of-Service (DoS) Attack

A Denial-of-Service (DoS) attack seeks to make a system or service inaccessible by bombarding it with huge amounts of traffic or requests so that it cannot respond to authentic users. Attackers can flood web servers, networks, or applications, which results in performance slowdown, downtime, and financial losses. Two frequent types are volumetric attacks (bandwidth overloading) and application-layer attacks (focusing on particular apps or services).

Control Mechanisms:

It is essential to have network firewalls and IPS configured to detect and block suspicious traffic. Organizations can deploy rate limiting to limit the number of incoming requests that can be handled by a server at a time. Specialized DDoS mitigation services such as Cloudflare or Akamai provide filtering and absorption of unwanted traffic before it reaches the target. Active monitoring of the network for unusual traffic flow allows for early detection and mitigation. Example: The massive DDoS attack on Dyn in 2016 caused massive outages for websites including Twitter, Netflix, and Reddit (Scarfone and Mell, 2007).

3. SQL Injection



SQL Injection (SQLi) is a web application attack that allows an attacker to inject malicious SQL code into queries sent by an application to its database. Vulnerable input fields like login pages or search boxes are targeted by attackers and injected with malicious SQL code to manipulate the database. This can lead to unauthorized access, data leakage, data modification, or even complete deletion of sensitive information.

Control Mechanisms:

The most optimal approach to prevent SQL Injection is to use parameterized queries and prepared statements at the time of application development. Input sanitization and validation must be performed for every piece of user-input information. Web Application Firewalls can detect and block suspicious patterns of SQL queries. Furthermore, the concept of least privilege applied to database accounts minimizes the effect of an attack. Example: The notorious Heartland Payment Systems breach in 2008 was due to an SQL Injection vulnerability that exposed millions of credit card numbers (OWASP Foundation, 2021).

4. Zero-Day Exploit

Zero-day attacks are founded on undiscovered bugs in software, hardware, or firmware that the vendor has not yet had a way to correct. The attackers can exploit the vulnerabilities as soon as they have been discovered before the developers are aware of the issue, exposing organizations to vulnerabilities. Zero-day threats are typically used in advanced persistent threats (APTs) against valuable systems.

Control Mechanisms:

Utilizing Endpoint Detection and Response (EDR) tools that search for anomalous behaviors, as compared to signature detection, can help in the detection of zero-day exploitation. Software has to be up-to-date, possess a good patching policy, and make use of threat intelligence feeds to stay informed about emerging threats. Scheduled vulnerability scans also help to minimize attack surfaces. Example: In 2021, a Microsoft Exchange Server zero-day exploit campaign took advantage of thousands of organizations worldwide, rendering emails and sensitive data accessible to attackers for stealing (Symantec, 2020).

5. DNS Tunneling

DNS tunneling is an attack method whereby attackers encapsulate malware traffic or data exfiltration in DNS queries and responses. Since DNS is a highly trusted protocol and usually permitted through firewalls without intrusive inspection, attackers exploit it to tunnel around network security controls and create hidden communication channels to command-and-control (C2) servers.

Control Mechanisms:

Examining DNS traffic for abnormalities, such as excessive DNS queries or misformatted domain names, can detect DNS tunneling. Organizations need to have DNS firewalls that can filter known malicious domains and conduct deep packet inspection of DNS traffic. Security Information and Event Management (SIEM) systems can also be set up to trigger alerts on suspicious DNS patterns. Example: Several cyberespionage campaigns in 2019 used DNS

tunneling techniques for exfiltrating sensitive government and enterprise data (Trend Micro Research, 2020).

PART B: Practical Network Packet Analysis – Wireshark

Methodology

The analysis was performed through a detailed examination of several .pcap files with the help of Wireshark, a widespread network protocol analyzer. The methodology was focused on identifying strange traffic patterns, malicious packets, and probable signs of attack activity.
In Wireshark, specific filter syntax was employed to restrict relevant traffic:

- For FTP traffic analysis:
  ftp.request.command == "USER" || ftp.request.command == "PASS"
- For DNS analysis:
  Dns
- For SSL/TLS examination:
  Ssl
- For anomalies in Wi-Fi networks:
  wlan.fc.type_subtype == 8 (Beacon frames)

The host and traffic analysis stages encompassed close examination of packet headers, monitoring handshake procedure, detecting duplicated or spurious requests, and identification of plaintext transmission of credentials.

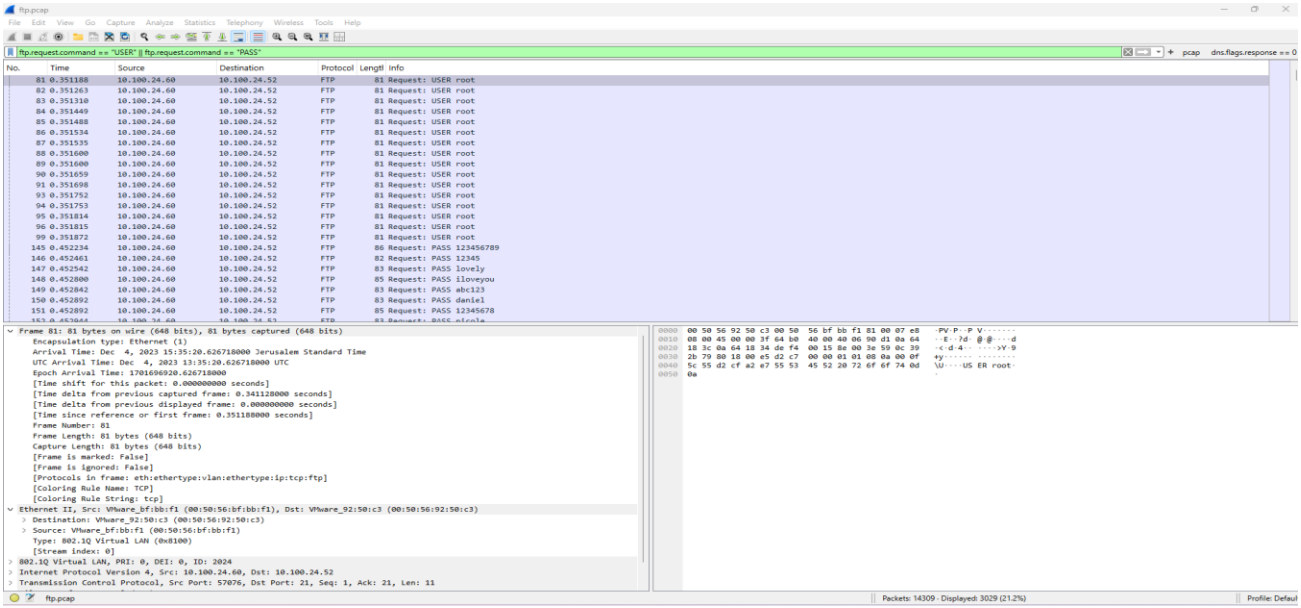
Analysis involved and employed tools and techniques for the following:

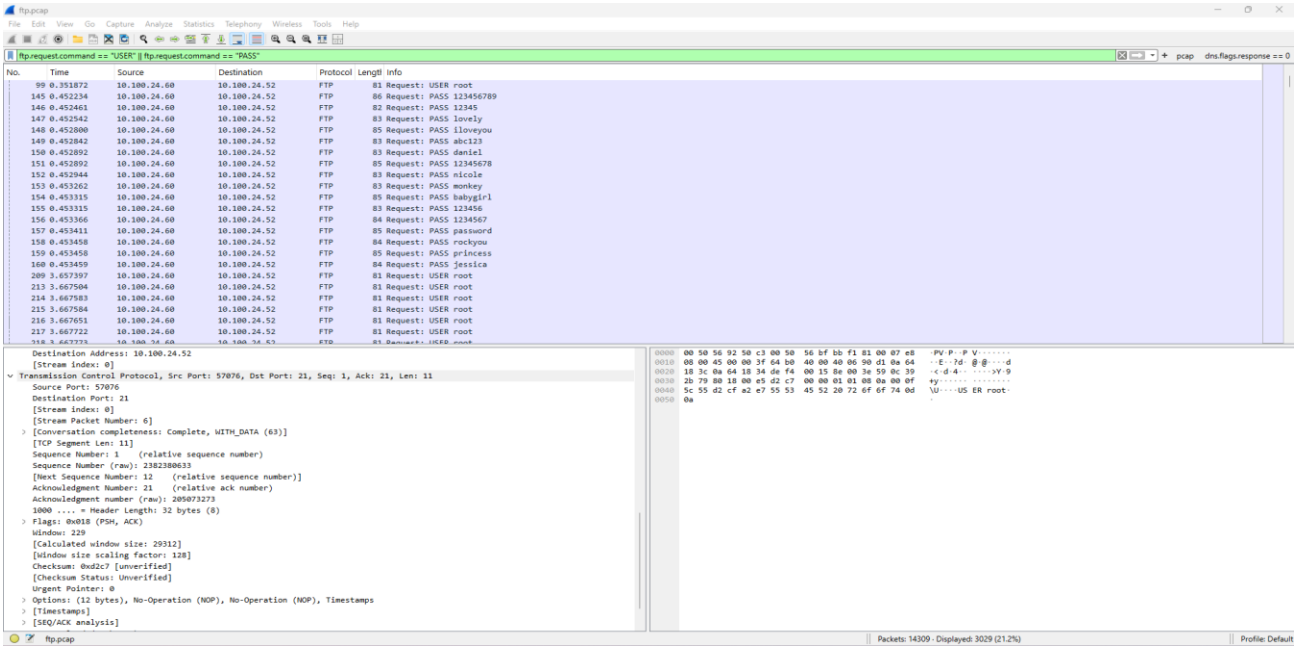
- Wireshark filters to exclude protocols.
- TCP stream analysis for FTP credential exposure.
- DNS query analysis for tunneling activity.
- SSL/TLS handshake analysis for abnormal behavior.
- 802.11 management frame analysis for wireless network attacks.

All suspicious results were validated through detailed packet analysis to ensure accuracy and relevance to the attack categories in question.

Screenshots were captured as proof, and observations were recorded for each attack found.

Network Attack 1: (FTP Credential Theft)





Upon analysis of ftp.pcap, FTP login attempts were observed to transmit usernames and passwords in plaintext. Wireshark showed commands like USER root and PASS 12345678, revealing unencrypted credential exchanges. FTP is an insecure protocol by nature as it does not

encrypt traffic. Attackers sniffing these packets on an insecure network would easily obtain login credentials and gain unauthorized access.

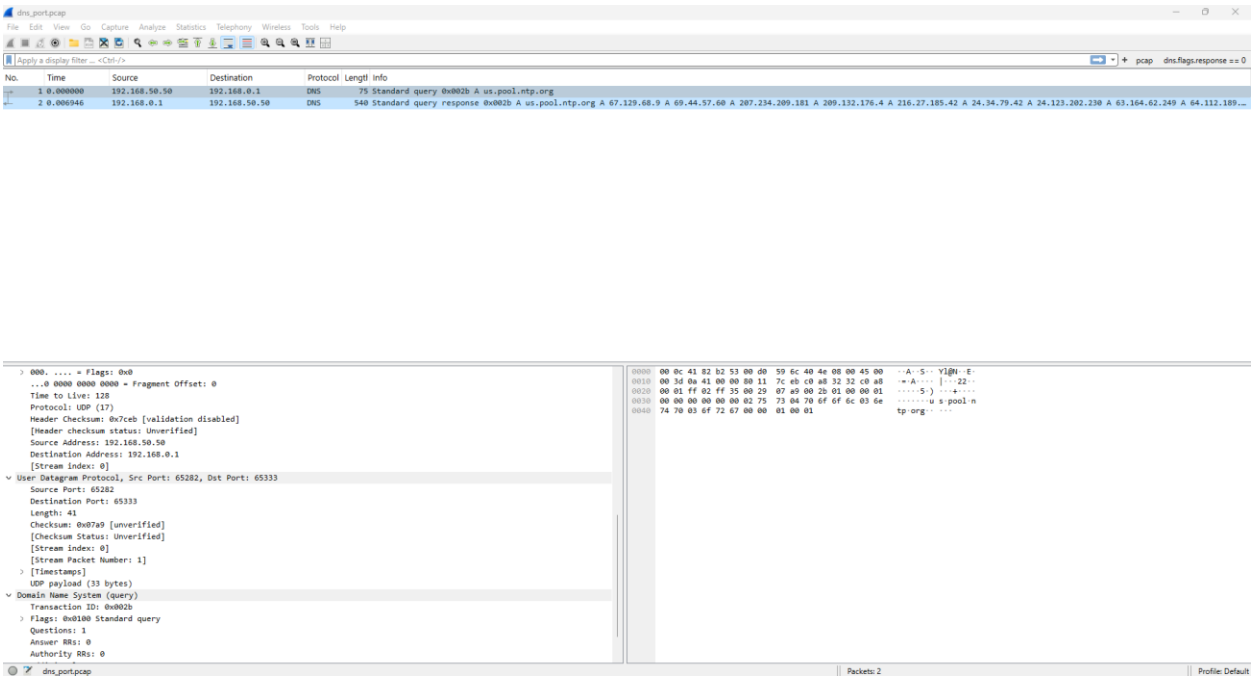
Packet-Level Information:

Captured FTP packets showed that the USER and PASS commands were transmitted in plaintext without any encryption. When the packet payloads were analyzed, login details such as passwords and usernames were clearly visible in the application data area. This lack of encryption exposes the sensitive information to interception from any network-monitoring attacker.

Observation:

Credentials exposed in cleartext expose the system to unauthorized login, account hijacking, and potential lateral movement in the network.

Network Attack 2: (DNS Query Abnormality)



In the dns_port.pcap file, unusual DNS queries were found. One DNS query to us.pool.ntp.org returned multiple IP addresses, many more than typical for a time synchronization service.

This kind of activity can be a sign of DNS tunneling, when attackers insert payloads within DNS traffic to evade detection by firewalls and drain data or establish covert channels.

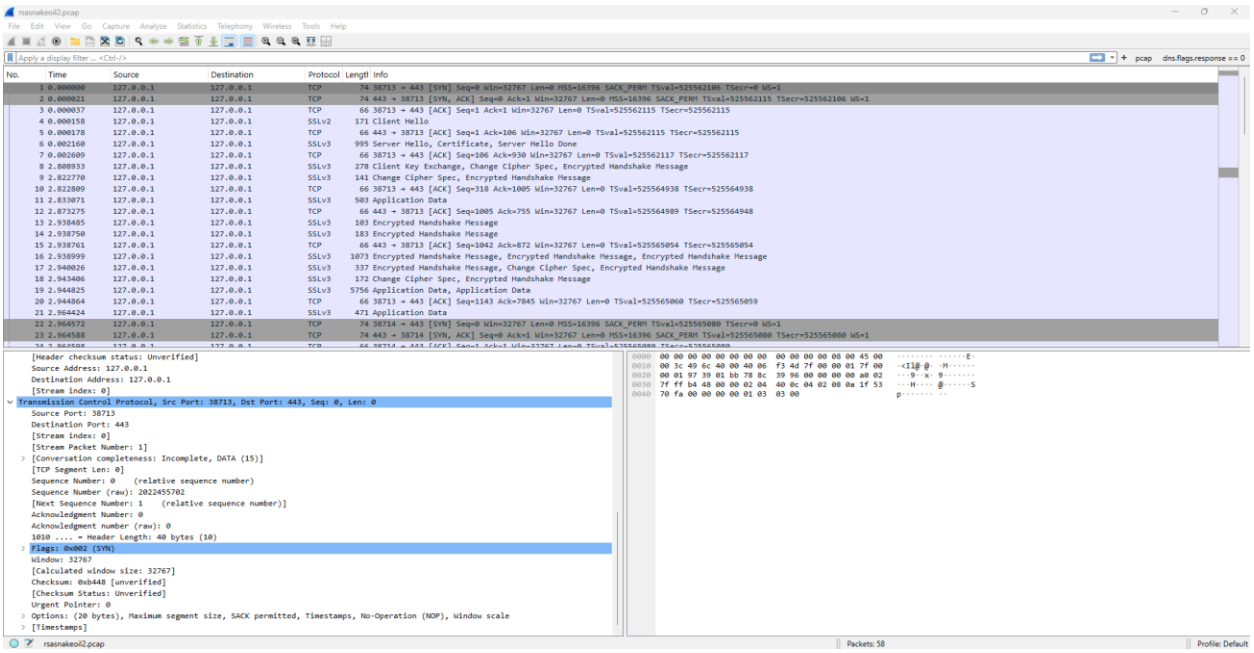
Packet-Level Details:

DNS query and response packet analysis identified abnormally long responses containing multiple A records (IPv4 addresses) within a single response. DNS responses typically are brief with one or multiple IP addresses. Multiple IP addresses or extremely long DNS names were indicative of the presence of DNS tunneling activity intended to bypass conventional security controls.

Observation:

DNS queries are usually brief and small. Big chunks or responses with huge numbers of IP addresses are unusual and need closer scrutiny.

Network Attack 3: (SSL/TLS Encrypted Attack Attempts)



Analysis of rsanakoeil2.pcap revealed repeated SSL/TLS handshake attempts between the same hosts at close intervals. Although encryption is meant to secure communication, repeated or irregular patterns of handshakes are a sign of evasion attempts or encrypted command-and-control (C2) communication.

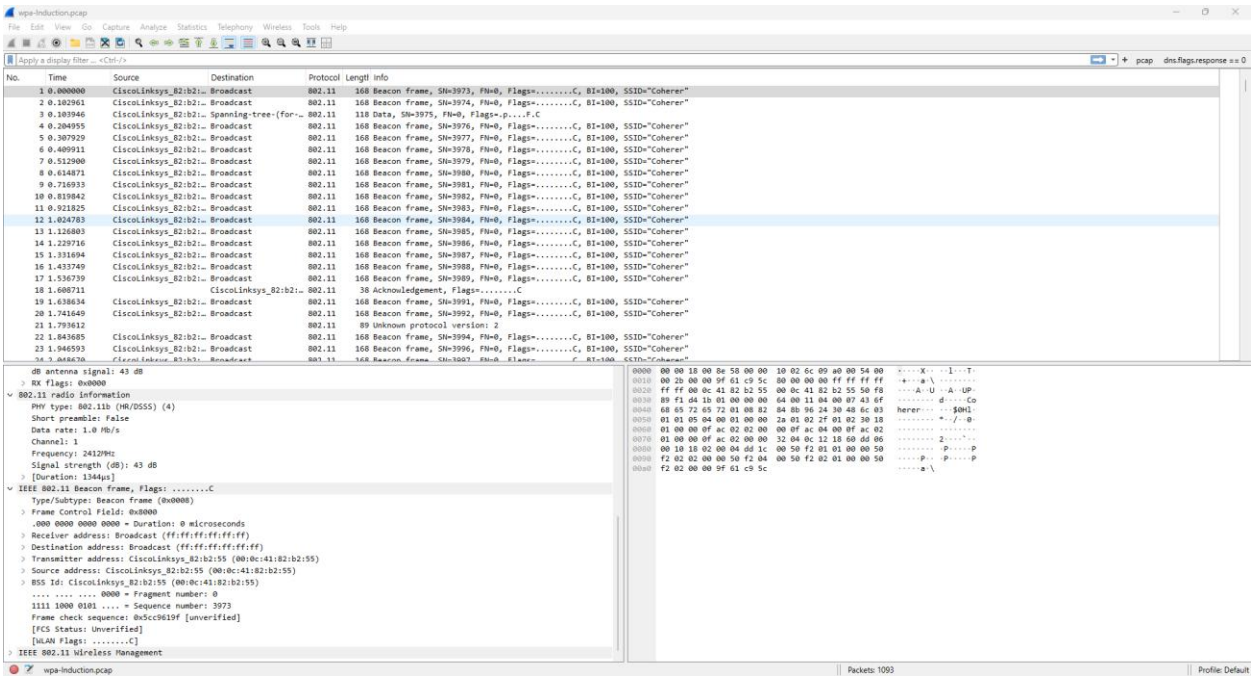
Packet-Level Details:

Packet analysis was focused on SSL handshake messages, namely Client Hello and Server Hello. Multiple handshake attempts were observed between the same client and server IP addresses within short time intervals but with few successful established sessions. Session ID values were not the same, and repeated renegotiation attempts pointed toward potential abuse of SSL/TLS protocols for creating hidden communication tunnels.

Observation:

Excessive and failed SSL/TLS handshakes can be a sign that an attacker is attempting to hide malicious traffic in encrypted tunnels, avoiding detection.

Network Attack 4: (Wi-Fi Beacon Flood Attack)



In the wpa-induction.pcap, a Wi-Fi beacon flood attack was detected. There were thousands of beacon frames announcing the SSID "Coherer" in a short period. This attack is designed to overwhelm clients by flooding the wireless space with spoofed access points, causing network instability or denial-of-service (DoS) for legitimate clients.

Packet-Level Details:

Captured Wi-Fi traffic showed a lot of number of Beacon frames being sent. Inside each Beacon frame were different spoofed SSIDs being broadcast from the same or similar MAC addresses. Whereas a Wi-Fi access point will normally send periodic Beacon frames to announce its presence, in this instance, the number and rapid sending of fake Beacons immediately indicated that this was an intentional attempt to flood the wireless spectrum and disrupt legitimate Wi-Fi networks.

Observation:

Flooding of beacon frames can deplete device resources, disrupt connectivity, and open the door to man-in-the-middle attacks.

Conclusion

Hands-on analysis identified some of the real-world cyber threats of today, which can be detected using Wireshark. Identification of FTP plaintext credential stealing, suspicious DNS activity, unethical SSL/TLS handshakes, and Wi-Fi beacon flooding demonstrates how packet analysis is necessary in today's cybersecurity. Organizations must use proper encryption, monitor network traffic, secure DNS communications, and deploy wireless protection to thwart such attacks. Continuous packet-level scanning using tools like Wireshark can significantly improve an organization's defense against ever-evolving cyber threats.

References

Rouse, M. (2020) *Man-in-the-middle attack (MITM)*. TechTarget. Available at: https://www.techtarget.com (Accessed: 27 April 2025).

Scarfone, K. and Mell, P. (2007) *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Gaithersburg, MD: National Institute of Standards and Technology (NIST).

OWASP Foundation (2021) *SQL Injection*. Available at: https://owasp.org/www-community/attacks/SQL_Injection (Accessed: 27 April 2025).

Symantec (2020) *What is a Zero-Day Vulnerability?* Available at: https://www.broadcom.com/company/newsroom/press-releases?filtr=Security (Accessed: 27 April 2025).

Trend Micro Research (2020) *DNS Tunneling Threat Report*. Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/dns-tunneling-how-it-works-and-how-to-detect-it (Accessed: 27 April 2025).