www.codelivly.com

TOP 23

WIRESHARK FILTERS

for Threat Detection

CODELIVLY
LEARN CYBERSECURITY

WHAT IS WIRESHARK?

Wireshark is a widely-used open-source network protocol analyzer.

Purpose

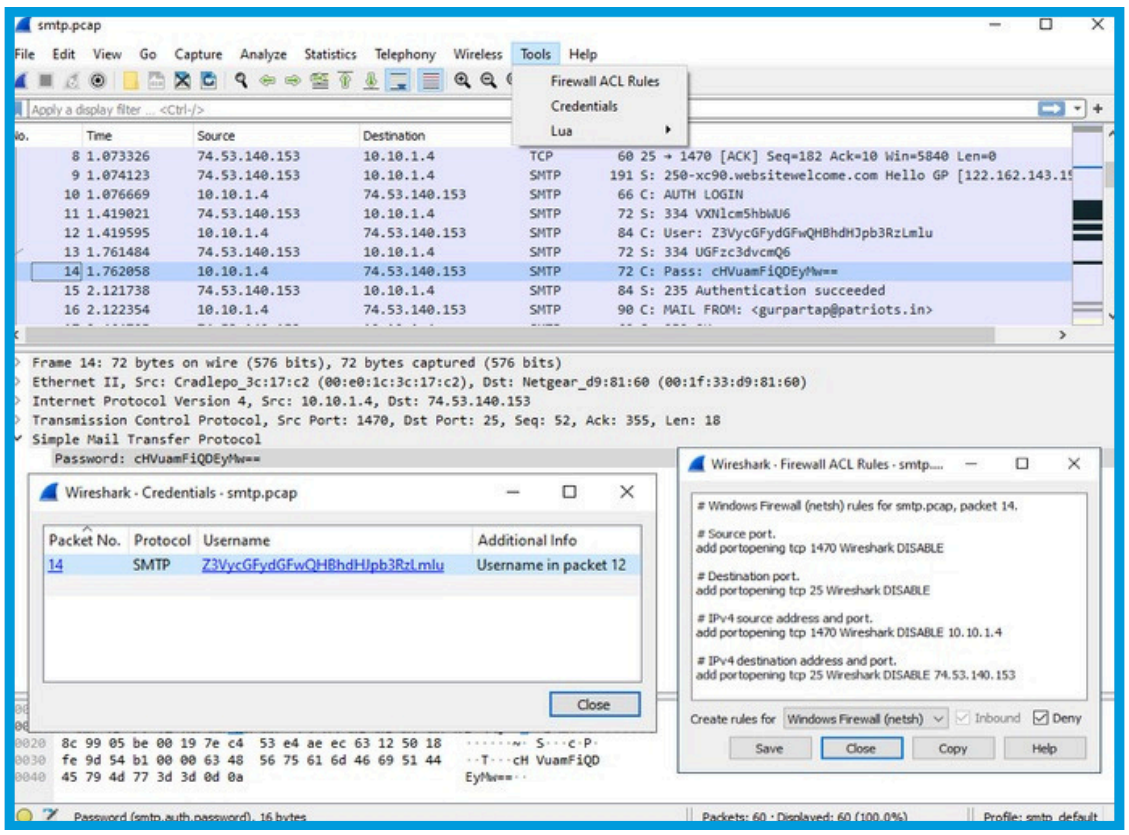
It captures and analyzes network traffic in real-time, helping in troubleshooting, security analysis, and network optimization.

Key Features:

- **Deep inspection of hundreds of protocols.**
- **Live traffic capture and offline analysis.**
- **Ability to decrypt many protocols, including SSL/TLS.**

WHY USE WIRESHARK?

- Network Troubleshooting: Identify network issues, bottlenecks, and performance problems.
- Security Analysis: Detect malicious activities, such as malware, DDoS attacks, and suspicious traffic.
- Protocol Development: Assist developers in debugging protocol implementations.
- Real-Time Monitoring: Monitor network data in real-time for quick response to anomalies.



WIRESHARK FILTERS

What are Filters?

Filters in Wireshark help narrow down specific traffic of interest from a large dataset.

Types of Filters:

- **Capture Filters: Applied during data capture, limiting the data being captured.**
- **Display Filters: Applied after capturing data, allowing for in-depth analysis of specific traffic.**

Common Display Filter Examples:

- **IP Filter: ip.addr == 192.168.1.1 (Shows traffic to/from a specific IP address)**
- **Port Filter: tcp.port == 80 (Shows traffic on a specific port, like HTTP)**
- **Protocol Filter: http (Displays HTTP protocol traffic)**

TOP 23 WIRESHARK FILTERS

1

HTTP GET FLOODING

How does the threat work?

Attackers generate a high volume of HTTP GET requests, overloading the server's capacity, causing denial of service.

Display filter

```
http.request.method == "GET"
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check the HTTP headers for an abnormal number of requests from the same source IP.**
- **If the source IP varies, investigate suspicious patterns in user-agent strings.**

2

DNS TUNNELING

How does the threat work?

DNS queries are manipulated to transmit data, bypassing firewalls and performing covert data exfiltration.

Display filter

```
dns
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Inspect the DNS query field for abnormal payload sizes or repeated requests.**
- **For high-frequency DNS queries from one source, analyze the DNS response time for unusual delays.**

3

SMB BRUTE FORCE

How does the threat work?

Multiple login attempts are made via the SMB protocol, trying to guess valid credentials through repetitive trials.

Display filter

```
smb.cmd == 0x73
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check the SMB headers for failed login attempts in the status code field.**
- **If the attack includes successful logins, monitor SMB command response times.**

4

SYN FLOOD ATTACK

How does the threat work?

Attackers flood the target server with SYN packets without completing the TCP handshake, exhausting server resources.

Display filter

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

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review the TCP headers and check if there's a high volume of SYN packets without corresponding ACKs.**
- **If there are some ACK responses, look for unusually delayed ACKs or connection resets.**

5

DNS AMPLIFICATION

How does the threat work?

Attackers use a small request to trigger large DNS responses, reflecting traffic back to the target and overwhelming it.

Display filter

```
dns.qry.name
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check the DNS response section for large-sized responses and unexpected source addresses.**
- **If response sizes seem normal, look at the TTL field for unusually low values.**

6

ICMP FLOODING (PING OF DEATH)

How does the threat work?

The attacker sends numerous ICMP requests (pings) to overload a device, consuming bandwidth and resources.

Display filter

```
icmp
```

How to detect?

- Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.
- Review the ICMP headers for a high frequency of Echo Request packets from a single source.
- If packet sizes are unusual, inspect for ICMP packets larger than the standard 64 bytes.

7

ARP SPOOFING

How does the threat work?

An attacker sends falsified ARP messages, leading devices to link wrong MAC addresses with IP addresses.

Display filter

```
arp.duplicate-address-frame
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Inspect the ARP header for mismatches between IP and MAC addresses.**
- **If there are no clear mismatches, check for ARP requests with identical source IPs but different MAC addresses.**

8

DNS POISONING

How does the threat work?

DNS responses are altered or forged to redirect users to malicious websites instead of legitimate ones.

Display filter

```
dns.flags.rcode != 0
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Analyze DNS response headers for mismatched IP addresses or altered TTL values.**
- **If there's no direct mismatch, check the response time field for unexpected delays.**

9

SUSPICIOUS HTTP USER-AGENT

How does the threat work?

Attackers may use irregular User-Agent strings to mask their identity or avoid detection during attacks.

Display filter

```
http.user_agent
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Examine the HTTP headers for unusual or malformed User-Agent strings.**
- **If the User-Agent is not obviously suspicious, correlate requests with known malicious IP addresses.**

10

FTP PLAINTEXT AUTHENTICATION

How does the threat work?

FTP transmits login credentials in plaintext, making them vulnerable to interception by attackers.

Display filter

```
ftp.request.command == "USER"
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review FTP request headers for visible usernames and passwords.**
- **If no clear credentials are visible, inspect packet payloads for plaintext data in the FTP stream.**

11

BRUTE FORCE LOGIN (SSH)

How does the threat work?

Attackers repeatedly attempt to guess valid SSH credentials, exploiting weak or default passwords.

Display filter

```
ssh
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Look for repetitive login attempts in the SSH connection handshake fields.**
- **If there are fewer attempts, analyze the session duration for failed vs successful logins.**

12

DHCP STARVATION ATTACK

How does the threat work?

Attackers request multiple DHCP leases, depleting available IP addresses to prevent legitimate network access.

Display filter

```
dhcp
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Analyze the DHCP transaction ID for a high number of requests without corresponding DHCP Offers.**
- **If offers are present, check for quick lease time expiration in the DHCP header.**

13

SUSPICIOUS TLS CERTIFICATE

How does the threat work?

Attackers use invalid or self-signed TLS certificates to compromise encrypted communications.

Display filter

```
ssl.handshake.type == 11
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review the SSL handshake header for certificates signed by unknown authorities.**
- **If the certificate seems valid, verify the encryption protocol used for downgrade attempts.**

14

TELNET CLEARTEXT TRANSMISSION

How does the threat work?

Telnet transmits all data, including passwords, in plaintext, making it easily interceptable by attackers.

Display filter

```
telnet
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check for visible login credentials in the Telnet data fields.**
- **If no credentials are visible, inspect for suspicious command execution strings in the payload.**

15

UNAUTHORIZED RDP ACCESS

How does the threat work?

Attackers attempt unauthorized access to a system via Remote Desktop Protocol (RDP) to take control of the system.

Display filter

```
tcp.port == 3389
```

How to detect?

- Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.
- Inspect RDP header fields for repeated connection attempts from the same IP.
- If the source IP changes, review session IDs for abnormal session initiation patterns.

16

PORT SCANNING

How does the threat work?

Attackers scan for open ports on a system to find vulnerabilities and identify services to exploit.

Display filter

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

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review the TCP flags in headers for SYN packets across different ports.**
- **If SYN-ACK responses are present, inspect for suspicious response delays or resets.**

17

SMTP EXFILTRATION

How does the threat work?

Sensitive information is extracted from a network by sending it out via email using the SMTP protocol.

Display filter

```
smtp
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review SMTP headers for large or abnormal email attachments.**
- **If attachment size seems normal, inspect destination domains for unauthorized or unknown email addresses.**

18

ROGUE DHCP SERVER

How does the threat work?

A rogue DHCP server assigns unauthorized IP addresses, redirecting network traffic or causing denial of service.

Display filter

```
dhcp
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review the DHCP Offer packets and compare the DHCP server IP address to authorized DHCP servers.**
- **If server IPs match, check for abnormal lease durations or lease renewals in the DHCP headers.**

19

SQL INJECTION ATTACK

How does the threat work?

Malicious SQL code is injected into vulnerable input fields, granting attackers unauthorized access to the database.

Display filter

```
http.request.uri contains "SELECT"
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review HTTP request URIs for SQL commands like SELECT, DROP, or INSERT within the URL or payload.**
- **If no SQL commands are found, inspect HTTP headers for error responses that could indicate failed injection attempts.**

20

VOIP EAVESDROPPING (SIP)

How does the threat work?

Attackers intercept Voice over IP (VoIP) traffic, allowing them to listen in on private conversations.

Display filter

```
sip
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check the SIP headers for unauthorized call setups or unknown user IDs initiating the call.**
- **If calls seem normal, analyze the RTP streams for abnormal traffic patterns or packet loss**

21

MALWARE COMMAND & CONTROL TRAFFIC

How does the threat work?

Malware communicates with a Command & Control (C2) server to receive instructions for further malicious activity.

Display filter

```
http contains "cmd.exe"
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review the HTTP request payloads for command execution instructions such as cmd.exe.**
- **If no commands are found, check for suspicious external server connections, especially to uncommon IPs.**

22

SSL DOWNGRADE ATTACK

How does the threat work?

Attackers force the use of weaker SSL/TLS encryption protocols, reducing security and allowing for interception or decryption.

Display filter

```
ssl.record.version < 0x0303
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Check the SSL/TLS handshake headers for negotiation with older protocol versions like SSL 2.0 or 3.0.**
- **If SSL/TLS versions are acceptable, inspect certificate chains for self-signed or expired certificates.**

23

SUSPICIOUS HTTP POST REQUESTS

How does the threat work?

Attackers use HTTP POST requests to upload files or send data to a server, which may be used for data exfiltration or malicious uploads.

Display filter

```
http.request.method == "POST"
```

How to detect?

- **Open Wireshark, navigate to the filter bar, and enter the above-mentioned display filter.**
- **Review HTTP headers for POST requests with unusually large payloads or requests to unknown IP addresses.**
- **If payload sizes are small, inspect the content of the POST body for base64-encoded or binary data.**

CONCLUSION

In conclusion, using Wireshark with targeted filters allows for effective threat detection and network security monitoring.

- Flexible tool: Wireshark adapts to various threats.
- Real-time detection: Spot suspicious traffic instantly.
- Layered insight: Analyze threats across multiple layers.
- Proactive defense: Identify attacks early to prevent damage.
- Customizable filters: Tailor filters to reduce false positives.
- Continuous updates: Stay prepared with regular Wireshark improvements.