

Wireshark: Traffic Analysis

## **Wireshark: Traffic Analysis – Full Report**

### **Task 1 – Introduction**

The objective of this lab was to practice real-world network traffic analysis using **Wireshark**. We analyzed packet captures for various scenarios, including reconnaissance, ARP poisoning, tunneling, cleartext protocol leaks, and encrypted traffic inspection. Each task focused on identifying malicious activity or extracting key forensic evidence.

### **Task 2 – Nmap Scans**

**Goal:** Detect and analyze reconnaissance activities performed using Nmap.

**Key Findings:**

* **Scan Type Detected:** TCP SYN and TCP Connect scans based on packet flags (SYN → SYN/ACK → RST).
* **Indicators:**
  + Rapid sequential port probes to multiple ports on a single host.
  + Nmap user agent in service banner grabs (e.g., HTTP headers).
* **Impact:** Reconnaissance phase of cyber kill chain, often preceding exploitation.

### **Task 3 – ARP Poisoning & Man In The Middle**

**Goal:** Identify ARP spoofing attempts.

**Key Findings:**

* **Evidence:** Multiple unsolicited ARP replies (“Who has X? Tell Y”) mapping attacker MAC to legitimate IP.
* **Result:** The attacker positioned themselves as a man-in-the-middle (MITM), intercepting victim-to-gateway traffic.
* **Impact:** Allows sniffing of sensitive data or injection of malicious payloads.

### **Task 4 – Identifying Hosts: DHCP, NetBIOS, and Kerberos**

**Goal:** Determine hosts and services in the network.

**Key Findings:**

* **DHCP:** Observed DHCP Discover and DHCP Offer packets revealing new host IP assignment.
* **NetBIOS:** Name service packets leaked workstation names and possibly logged-in user names.
* **Kerberos:** Kerberos authentication traffic to domain controllers revealed domain name and user principal names (UPNs).

### **Task 5 – Tunneling Traffic: DNS and ICMP**

**Goal:** Identify covert channels using legitimate protocols.

**Key Findings:**

* **DNS Tunneling:** Long TXT queries and unusual subdomain patterns (e.g., base64-encoded chunks).
* **ICMP Tunneling:** ICMP echo requests/replies with unusually large payloads carrying non-standard data.
* **Impact:** Used for bypassing firewalls, data exfiltration.

### **Task 6 – Cleartext Protocol Analysis: FTP**

**Goal:** Detect credentials and files transferred over FTP.

**Key Findings:**

* **FTP Authentication:** USER/PASS commands contained cleartext username/password.
* **File Transfer Evidence:** RETR and STOR commands indicated sensitive data movement.
* **Impact:** High risk if used over insecure networks.

### **Task 7 – Cleartext Protocol Analysis: HTTP**

**Goal:** Identify sensitive data in HTTP traffic.

**Key Findings:**

* **Extracted Info:** Login forms sent via POST with unencrypted credentials.
* **HTTP Headers:** User-Agent, Cookie values, and session tokens visible.
* **Impact:** Allows credential theft or session hijacking.

### **Task 8 – Encrypted Protocol Analysis: Decrypting HTTPS**

**Goal:** Analyze HTTPS traffic using provided keys.

**Key Findings:**

* Imported SSL keys into Wireshark to decrypt TLS streams.
* Identified URLs visited, login credentials, and form submissions that were originally encrypted.
* **Impact:** If private keys are compromised, full HTTPS confidentiality is lost.

### **Task 9 – Bonus: Hunt Cleartext Credentials**

**Goal:** Search across all traffic for credentials.

**Key Findings:**

* Used Wireshark filters:

ini

CopyEdit

http.request.method == "POST"

ftp.request.command == "USER" || ftp.request.command == "PASS"

* Found multiple plain text logins in FTP and HTTP.

### **Task 10 – Bonus: Actionable Results**

**Goal:** Produce security recommendations.

**Mitigation Recommendations:**

* Use encrypted protocols (SFTP, FTPS, HTTPS).
* Segment networks to limit MITM potential.
* Monitor DNS and ICMP for abnormal usage.
* Implement strict firewall rules to block tunneling.

### **Task 11 – Conclusion**

This lab demonstrated that **network traffic analysis** with Wireshark can uncover reconnaissance, MITM attacks, credential leaks, and covert channels. Unencrypted protocols were the easiest to analyze, while encrypted traffic required key material. The investigation reinforces the importance of encryption, network monitoring, and intrusion detection.

