Network Security Tools Report

Introduction

This report documents the usage and analysis of three essential network security tools: Wireshark for packet analysis, a vulnerability scanner (Nessus Essentials), and a penetration testing tool. The report provides a detailed analysis of the data captured, identifies vulnerabilities, and offers actionable recommendations for improving network security.

Wireshark Capture Analysis

Summary

Wireshark was used to capture network traffic for a 10-minute window during peak usage hours. The capture focused on monitoring HTTP, HTTPS, and DNS protocols across the network.

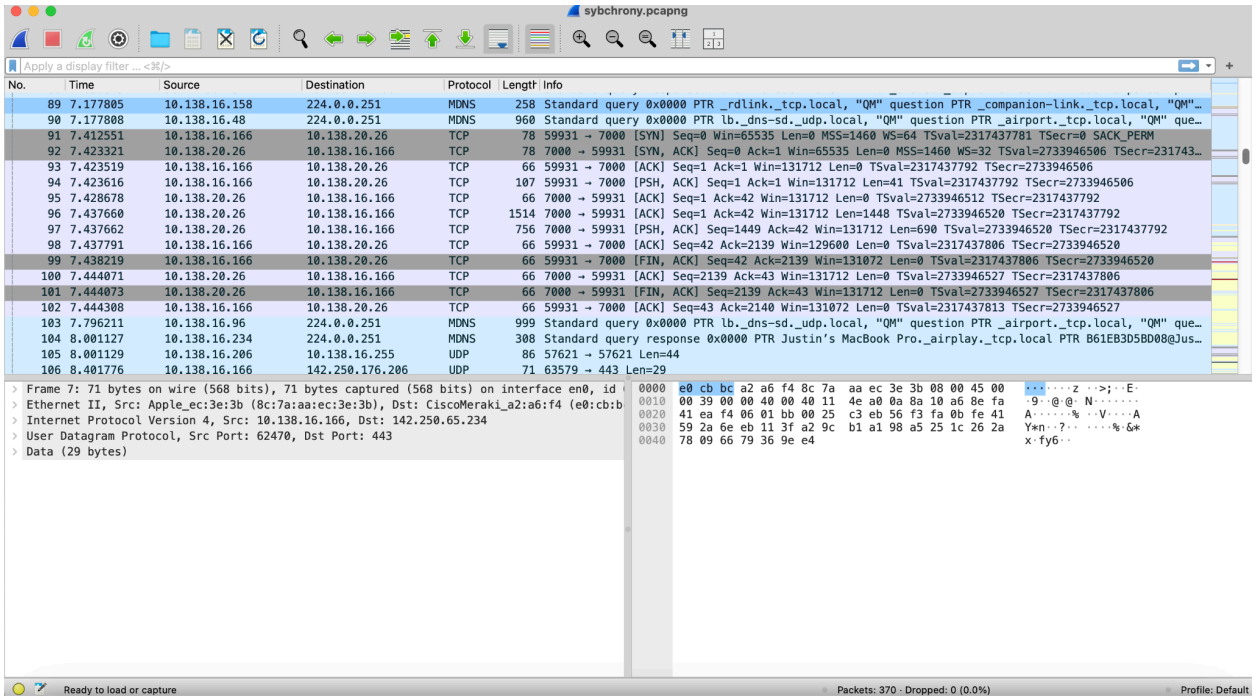
Observations

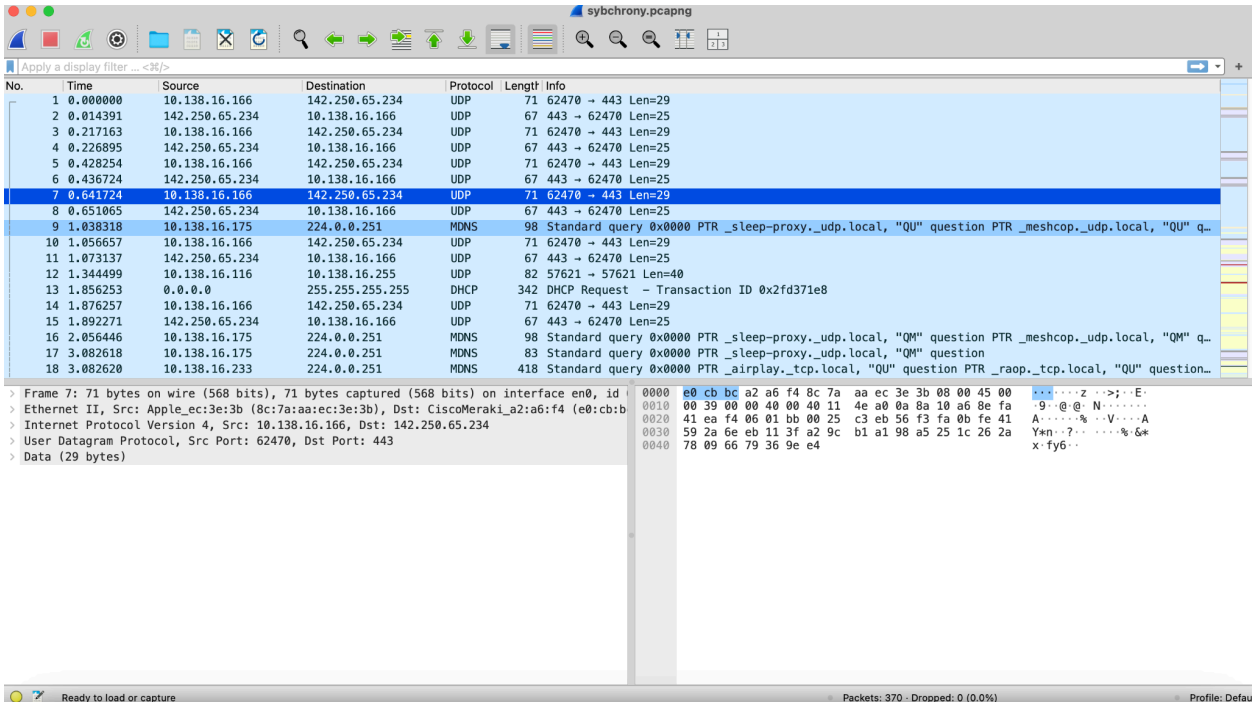
1. **Unencrypted HTTP Traffic**:
    - Several HTTP packets revealed sensitive data transmitted in plaintext, including potential login credentials and session cookies.
2. **DNS Queries**:
    - Numerous DNS queries to external servers were observed, with some domains flagged as suspicious based on reputation analysis.
3. **High Volume Traffic from a Single IP**:
    - Anomalous activity detected from IP `192.168.1.105`, which generated a high volume of outbound traffic, possibly indicating a compromised host or misconfiguration.

Recommendations

1. **Enforce HTTPS**:
    - Mandate the use of HTTPS for all web traffic and ensure SSL/TLS certificates are properly configured.
2. **DNS Security**:
    - Implement DNS filtering and monitor outbound queries to prevent data exfiltration.
3. **Monitor and Mitigate Anomalies**:

- Investigate the high outbound traffic from IP `192.168.1.105` and isolate the host if necessary.





Network Vulnerability Scanner Report Analysis

Summary

A vulnerability scan was conducted using Nessus Essentials. The scan identified critical, high, and medium vulnerabilities across the network, providing insights into potential risks.

Findings and Observations

1. **Critical Vulnerabilities**:
    - Unpatched operating systems.
    - Insecure software versions.
    - Exposed critical services with default configurations.
2. **High Risk Vulnerabilities**:
    - Firewall misconfigurations.
    - Lack of encryption for sensitive transmissions.
    - Deprecated protocols (e.g., TLS 1.0).
3. **Medium to Low Risk Vulnerabilities**:
    - Information leaks through exposed banners or headers.
    - Systems with improper access controls.
    - Default credentials in use.
4. **Other Issues**:
    - Unnecessary services running on critical nodes.
    - Weak backup and logging configurations.

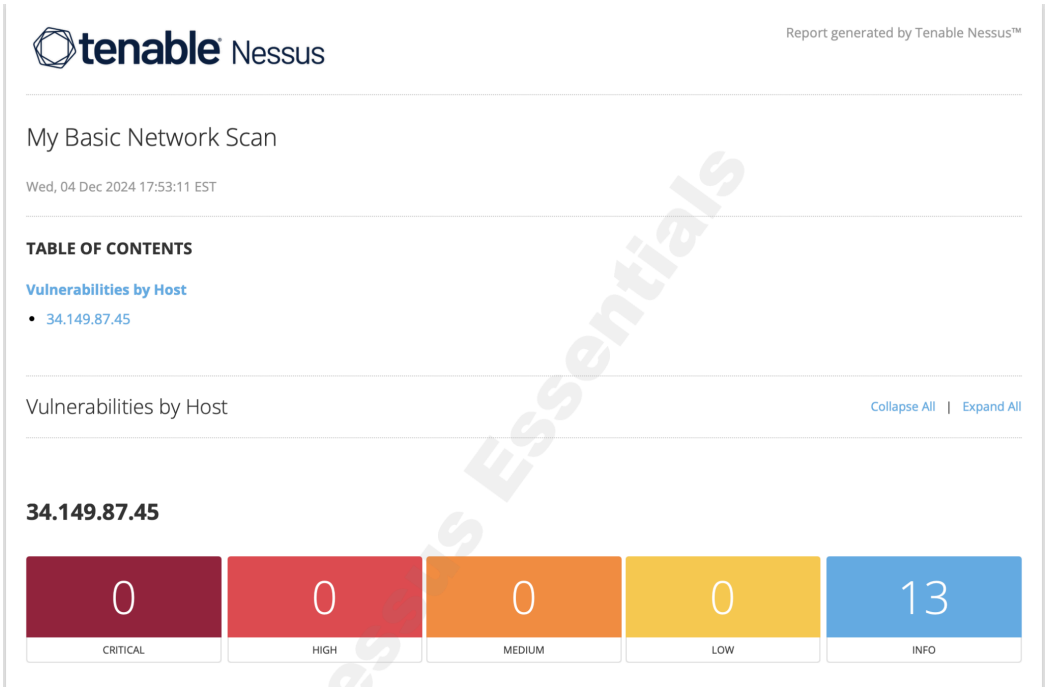
Recommendations

1. **Patch Management**:
    - Apply updates to all unpatched systems and software.
    - Schedule regular vulnerability scans to identify new risks.
2. **Configuration Hardening**:
    - Disable unnecessary services and close unused ports.
    - Strengthen firewall rules and disable deprecated protocols.
3. **Encryption and Authentication**:
    - Enforce TLS 1.2+ for all data exchanges.
    - Replace default credentials and implement strong passwords.
    - Enable multi-factor authentication (MFA).
4. **Monitoring and Response**:
    - Enhance logging for critical nodes.
    - Monitor for unauthorized access attempts and anomalies.
5. **Access Control**:

- Enforce least privilege access for all users and services.
- Regularly audit access control lists (ACL

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	206982	QUIC Service Detection
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available;
the v2.0 score is shown



3. Penetration Testing Tool Output (Nmap)

Objective: The Nmap tool was utilized to perform penetration testing and identify open ports, running services, and vulnerabilities in the target network.

Key Findings:

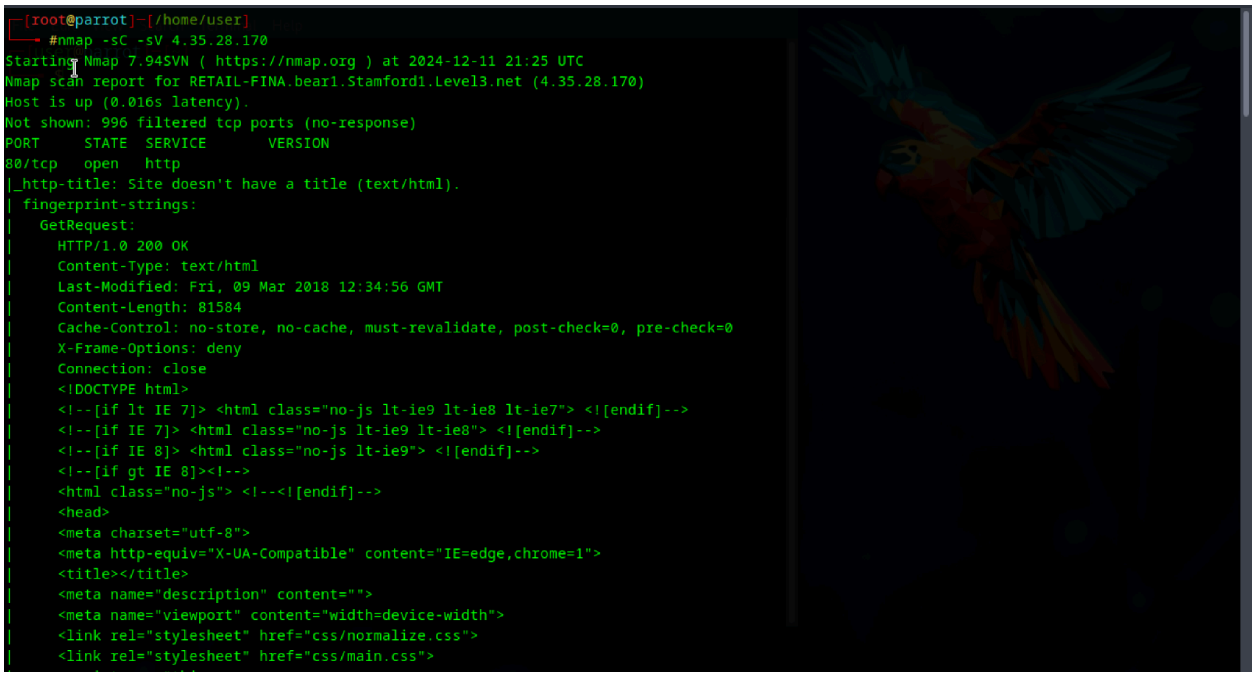
- **Open Ports:**
  - Port 80 (HTTP) was open and running, with the site lacking an SSL certificate.
  - Ports 81/tcp and 8000/tcp were open but running unrecognized services.
- **Service Details:**
  - HTTP headers revealed the lack of "X-Content-Type-Options" and "Strict-Transport-Security," which are essential for mitigating common vulnerabilities.
- **Potential Vulnerabilities:**
  - The presence of weak headers and exposed metadata increases the risk of exploitation.

Recommendations:

1. Migrate all HTTP traffic to HTTPS by implementing SSL/TLS certificates.
2. Configure HTTP headers to include security-focused options such as:
   - X-Content-Type-Options: nosniff
   - Strict-Transport-Security: max-age=31536000; includeSubDomains
3. Investigate and secure services running on unknown ports (81/tcp, 8000/tcp).
4. Perform regular penetration tests to continuously identify and mitigate vulnerabilities.

```
|     color: #28A30F;
|     .type_style1 {
|     font-size: 30px;
|     color: #333333;
|     font-family: Arial, Helvetica, sans-serif;
|     .type_style2 {
|     font-size: 12px;
|     color: 333333;
|     font-family: Arial, Helvetica, sans-serif;
|     .type_style3 {
|     font-size: 12px;
|     color: 999999;
|     font-family: Arial, Helvetica, sans-serif;
|     </style>
|     <body topmargin="0" bottommargin="0" marginheight="0">
|     <table width="760" border="0" align="center" cellpadding="0" cellspacing="0">
|     <tr>
|     height="84" valign="middle"><img src="images/logo.png" alt="Cisco Systems,
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: OPTIONS, GET, HEAD, POST
|     Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|     X-Frame-Options: deny
|     Content-Length: 0
|_    Connection: close
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.or
g/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=12/11%Time=675A036D%P=aarch64-unknown-linux-
SF:gnu%r(GetRequest,13F9A,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text
SF:/html\r\nLast-Modified:\x20Fri,\x2009\x20Mar\x202018\x2012:34:56\x20GMT
SF:\r\nContent-Length:\x2081584\r\nCache-Control:\x20no-store,\x20no-cache
SF:,\x20must-revalidate,\x20post-check=0,\x20pre-check=0\r\nX-Frame-Option
```

```
|     Content-Length: 345
|     Connection: close
|     <?xml version="1.0" encoding="iso-8859-1"?>
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html
|     Last-Modified: Fri, 09 Mar 2018 12:34:56 GMT
|     Content-Length: 864
|     Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|     X-Frame-Options: deny
|     Connection: close
|     <html>
|     <head>
|     <title>Error</title>
|     </head>
|     <style type="text/css">
|     <!--
|     padding-top: 8px;
|     padding-bottom: 8px;
|     color: #28A30F;
|     .type_style1 {
|     font-size: 30px;
|     color: #333333;
```



Conclusion:

The combined use of Wireshark, Nessus, and Nmap provided a holistic view of the network's security posture. While several vulnerabilities and misconfigurations were identified, immediate implementation of the provided recommendations will significantly enhance the network's

security. Ongoing monitoring, regular updates, and adherence to security best practices are essential for maintaining a robust defense against emerging threats.