

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

- Unencrypted HTTP Traffic:**
 - Several HTTP packets revealed sensitive data transmitted in plaintext, including potential login credentials and session cookies.
- DNS Queries:**
 - Numerous DNS queries to external servers were observed, with some domains flagged as suspicious based on reputation analysis.
- 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

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

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

The image displays two screenshots of the Wireshark network traffic analysis tool. The top screenshot shows a packet capture with a display filter of 'No.' and a list of packets. The bottom screenshot shows a packet capture with a display filter of 'No.' and a list of packets. Both screenshots show a mix of DNS, TCP, and UDP traffic.

Top Screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
89	7.177805	10.138.16.158	224.0.0.251	MDNS	258	Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" que...
90	7.177808	10.138.16.48	224.0.0.251	MDNS	960	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" que...
91	7.412551	10.138.16.166	10.138.20.26	TCP	78	59931 → 7000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2317437781 TSecr=0 SACK_PERM...
92	7.423321	10.138.20.26	10.138.16.166	TCP	78	7000 → 59931 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=2733946506 TSecr=231743...
93	7.423519	10.138.16.166	10.138.20.26	TCP	66	59931 → 7000 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2317437792 TSecr=2733946506
94	7.423616	10.138.16.166	10.138.20.26	TCP	107	59931 → 7000 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=41 TSval=2317437792 TSecr=2733946506
95	7.428678	10.138.20.26	10.138.16.166	TCP	66	7000 → 59931 [ACK] Seq=1 Ack=42 Win=131712 Len=0 TSval=2733946512 TSecr=2317437792
96	7.437660	10.138.20.26	10.138.16.166	TCP	1514	7000 → 59931 [ACK] Seq=1 Ack=42 Win=131712 Len=1448 TSval=2733946520 TSecr=2317437792
97	7.437662	10.138.20.26	10.138.16.166	TCP	756	7000 → 59931 [PSH, ACK] Seq=1449 Ack=42 Win=131712 Len=690 TSval=2733946520 TSecr=2317437792
98	7.437791	10.138.16.166	10.138.20.26	TCP	66	59931 → 7000 [ACK] Seq=42 Ack=2139 Win=129600 Len=0 TSval=2317437806 TSecr=2733946520
99	7.438219	10.138.16.166	10.138.20.26	TCP	66	59931 → 7000 [FIN, ACK] Seq=42 Ack=2139 Win=131072 Len=0 TSval=2317437806 TSecr=2733946520
100	7.444071	10.138.20.26	10.138.16.166	TCP	66	7000 → 59931 [ACK] Seq=2139 Ack=43 Win=131712 Len=0 TSval=2733946527 TSecr=2317437806
101	7.444073	10.138.20.26	10.138.16.166	TCP	66	7000 → 59931 [FIN, ACK] Seq=2139 Ack=43 Win=131712 Len=0 TSval=2733946527 TSecr=2317437806
102	7.444308	10.138.16.166	10.138.20.26	TCP	66	59931 → 7000 [ACK] Seq=43 Ack=2140 Win=131072 Len=0 TSval=2317437813 TSecr=2733946527
103	7.796211	10.138.16.96	224.0.0.251	MDNS	999	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question PTR _meshcop._udp.local, "QU" que...
104	8.001127	10.138.16.234	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR Justin's MacBook Pro._airplay._tcp.local PTR B61EB3D5B080@Jus...
105	8.001129	10.138.16.255	10.138.16.255	UDP	86	57621 → 57621 Len=44
106	8.401776	10.138.16.166	142.250.176.206	UDP	71	63579 → 443 Len=29

Bottom Screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
2	0.014391	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
3	0.217163	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
4	0.226895	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
5	0.428254	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
6	0.436724	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
7	0.641724	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
8	0.651065	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
9	1.038318	10.138.16.175	224.0.0.251	MDNS	98	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question PTR _meshcop._udp.local, "QU" q...
10	1.056657	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
11	1.073137	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
12	1.344499	10.138.16.116	10.138.16.255	UDP	82	57621 → 57621 Len=40
13	1.856253	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2fd371e8
14	1.876257	10.138.16.166	142.250.65.234	UDP	71	62470 → 443 Len=29
15	1.892271	142.250.65.234	10.138.16.166	UDP	67	443 → 62470 Len=25
16	2.056446	10.138.16.175	224.0.0.251	MDNS	98	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question PTR _meshcop._udp.local, "QM" q...
17	3.082618	10.138.16.175	224.0.0.251	MDNS	83	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question
18	3.082620	10.138.16.233	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" question...

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



Report generated by Tenable Nessus™

My Basic Network Scan

Wed, 04 Dec 2024 17:53:11 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 34.149.87.45

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

34.149.87.45



○

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">
<!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;

```

```

<script src="thir
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
RTSPRequest:
  HTTP/1.0 400 Bad Request
  Content-Type: text/html
  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>
81/tcp closed hosts2-ns
179/tcp closed bgp
8090/tcp open opsmessaging?
  fingerprint-strings:
    GenericLines:
      HTTP/1.0 400 Bad Request
      Content-Type: text/html
      Content-Length: 345

```

```

[~root@parrot]-[/home/user]
# nmap -sC -sV 4.35.28.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 21:25 UTC
Nmap scan report for RETAIL-FINA.bear1.Stamford1.Level3.net (4.35.28.170)
Host is up (0.016s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http
  _http-title: Site doesn't have a title (text/html).
  fingerprint-strings:
    GetRequest:
      HTTP/1.0 200 OK
      Content-Type: text/html
      Last-Modified: Fri, 09 Mar 2018 12:34:56 GMT
      Content-Length: 81584
      Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
      X-Frame-Options: deny
      Connection: close
      <!DOCTYPE html>
      <!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->
      <!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->
      <!--[if IE 8]> <html class="no-js lt-ie9"> <![endif]-->
      <!--[if gt IE 8]><!--
      <html class="no-js"> <!--<![endif]-->
      <head>
      <meta charset="utf-8">
      <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
      <title></title>
      <meta name="description" content="">
      <meta name="viewport" content="width=device-width">
      <link rel="stylesheet" href="css/normalize.css">
      <link rel="stylesheet" href="css/main.css">

```

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.