🌐 Network Testing Report

📄 Executive Summary

This phase of the project focused on identifying and analyzing network protocols, services, and traffic within a simulated lab environment using Parrot OS and Metasploitable 2. A combination of tools such as **Nmap**, **Wireshark**, and **enum4linux** were employed to uncover active services, test for vulnerabilities, and map out the network structure. Key services like FTP, SSH, and Telnet were detected, and traffic analysis revealed behavior patterns and potential security issues.

🔍 Protocol Testing

- **Action**: Ran Nmap service scan on `10.138.16.109`.
- **Result**: Identified open services:
    - `FTP (21)` - vsftpd 2.3.4
    - `SSH (22)` - OpenSSH 4.7p1
    - `HTTP (80)` - Apache 2.2.8
    - `Telnet (23)` - Linux telnetd
    - Others: SMTP, NetBIOS, NFS, Java RMI, etc.
- **Browser Check**: Visiting `http://10.138.16.109` reveals a vulnerable Metasploitable 2 homepage with links to:
    - TWiki
    - phpMyAdmin
    - Mutillidae
    - DVWA
    - WebDAV

These indicate the presence of deliberately vulnerable applications.

🛠️ Service Enumeration

- **Tool Used**: `enum4linux -a 10.138.16.109`
- **Findings**:
    - Enumerated shared resources
    - Identified workgroup info (WORKGROUP)
    - NetBIOS names and user details revealed
- **Purpose**: Gather insight into SMB service and potential users or misconfigurations.

🗺️ Network Mapping

- **Diagram**: (See Image Provided)
    - **Attacker Machine**: Parrot OS
    - **Target**: Metasploitable 2
    - **Discovered Services**: FTP, SSH, Telnet, HTTP

⚠️ Access Point Identification

Service	Port	Vulnerability	Risk Level	Why It's Risky
FTP	21	Anonymous login allowed	High	Unauthorized access without credentials
Telnet	23	Insecure remote login	High	Sends credentials in plaintext
HTTP	80	Apache 2.2.8 outdated, directory indexing enabled	High	Many known CVEs, info disclosure
SSH	22	OpenSSH 4.7p1 (old version)	Medium	May be vulnerable to brute-force or RCE exploits

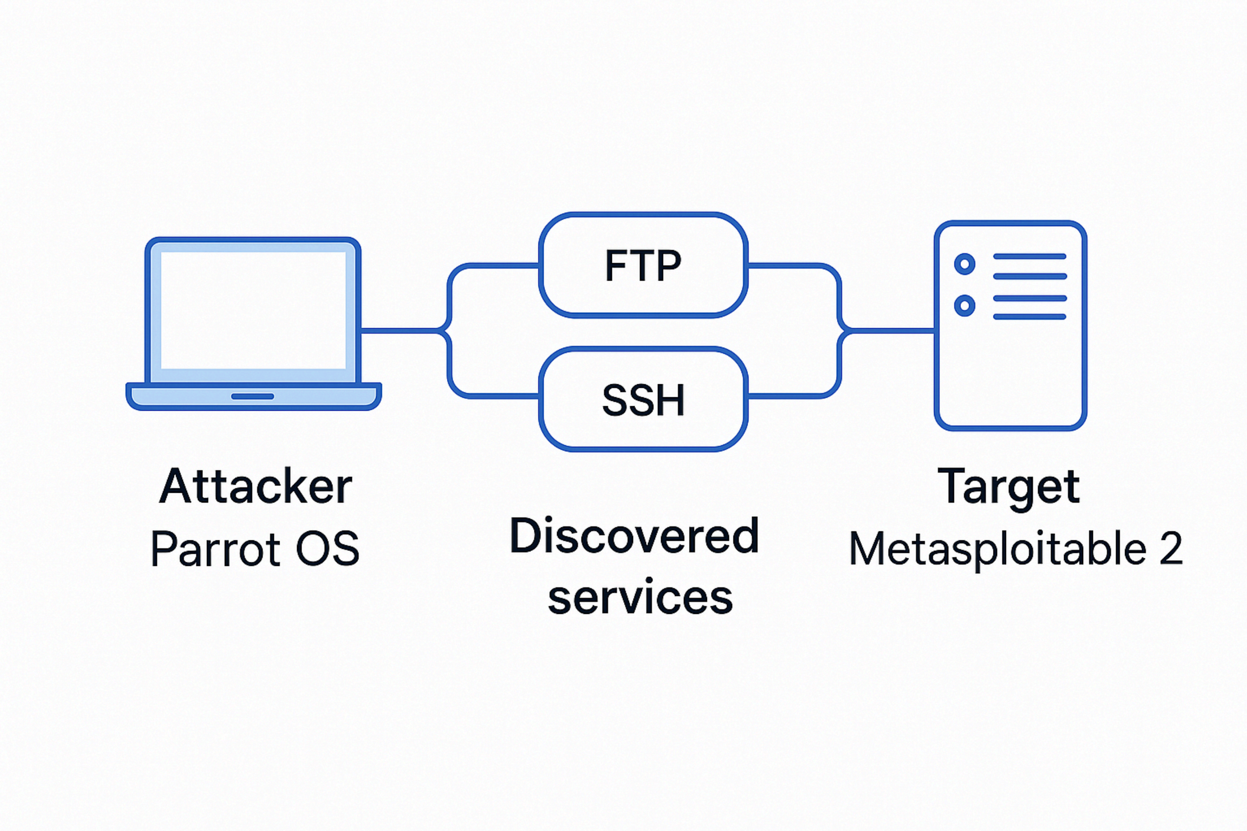
📡 Traffic Analysis

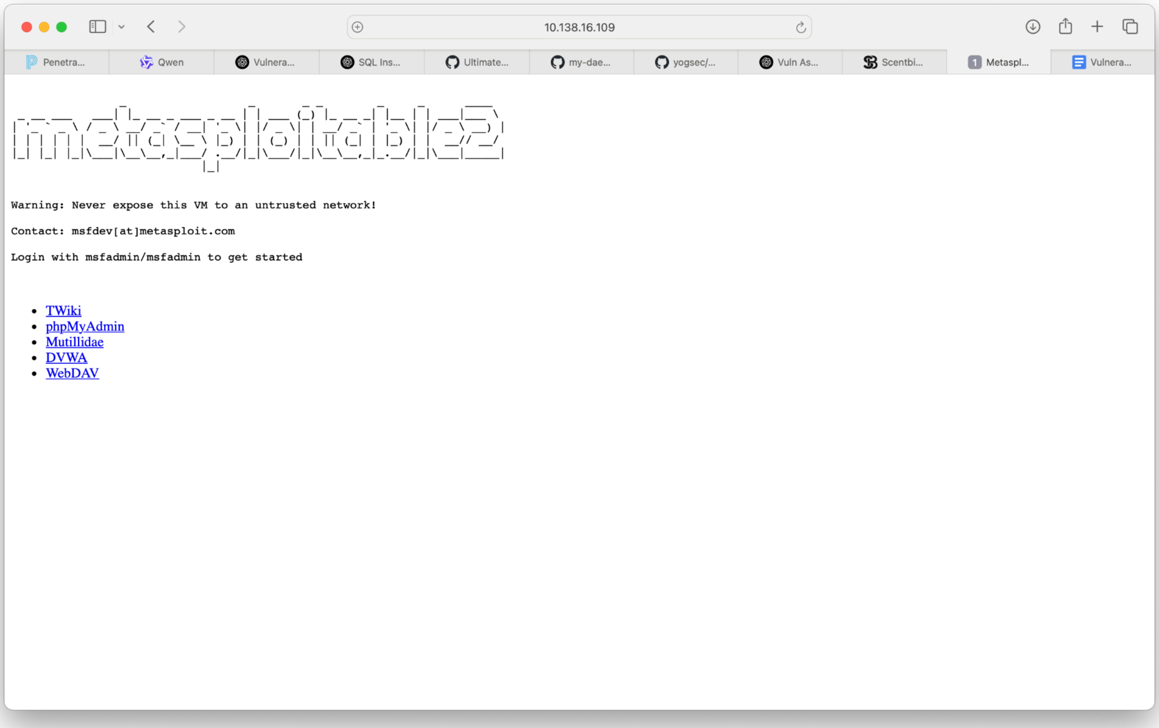
- **Tool Used**: Wireshark
- **Filter Applied**: `ip.addr == 10.138.16.109`
- **Captured Protocol**: ICMP (ping) traffic
- **Observation**: Echo requests and replies confirm live host and connectivity.
- **Insights**:
    - No encrypted traffic detected in ping
    - Highlighted the presence of unsecured and visible traffic
    - Useful for host discovery and timing analysis

✅ Recommendations

Risk Area	Suggested Mitigation

Anonymous FTP	Disable anonymous login or restrict access via firewall
Telnet	Replace with SSH or secure access layer (e.g., VPN)
Apache (HTTP)	Upgrade Apache version and disable directory indexing
Old OpenSSH	Update SSH server and enforce strong password policy
General	Segment network, monitor with IDS, apply least privilege





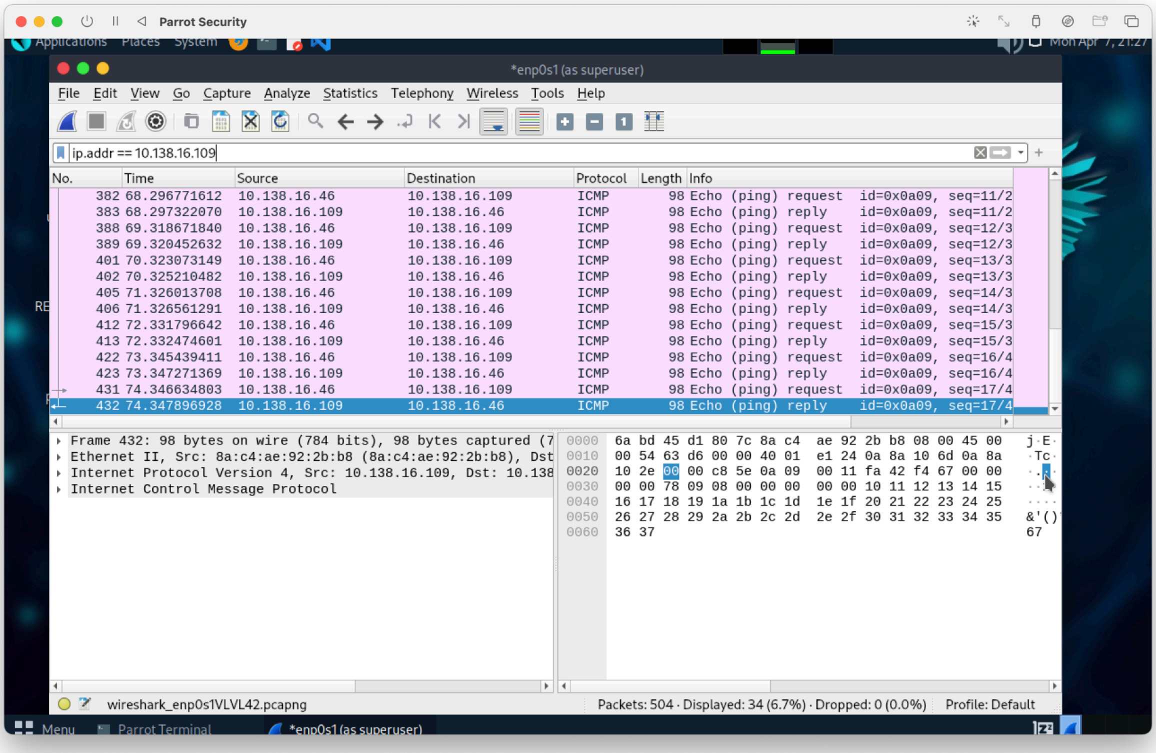
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV


Parrot Security
Applications Places System
Mon Apr 7, 21:27
*enp0s1 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Menu
Parrot Terminal
*enp0s1 (as superuser)

ip.addr == 10.138.16.109

```
No.   Time            Source          Destination     Protocol Length Info
  382 68.296771612 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=11/2
  383 68.297322070 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=11/2
  388 69.318671840 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=12/3
  389 69.320452632 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=12/3
  401 70.323073149 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=13/3
  402 70.325210482 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=13/3
  405 71.326013708 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=14/3
  406 71.326561291 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=14/3
  412 72.331796642 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=15/3
  413 72.332474601 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=15/3
  422 73.345439411 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=16/4
  423 73.347271369 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=16/4
  431 74.346634803 10.138.16.46    10.138.16.109   ICMP        98 Echo (ping) request  id=0x0a09, seq=17/4
  432 74.347896928 10.138.16.109   10.138.16.46    ICMP        98 Echo (ping) reply    id=0x0a09, seq=17/4
```

```
Frame 432: 98 bytes on wire (784 bits), 98 bytes captured (7
Ethernet II, Src: 8a:c4:ae:92:2b:b8 (8a:c4:ae:92:2b:b8), Dst
Internet Protocol Version 4, Src: 10.138.16.109, Dst: 10.138
Internet Control Message Protocol
```

```
0000  6a bd 45 d1 80 7c 8a c4  ae 92 2b b8 08 00 45 00   j·E·
0010  00 54 63 d6 00 00 40 01  e1 24 0a 8a 10 6d 0a 8a   ·Tc·
0020  10 2e 00 00 c8 5e 0a 09  00 11 fa 42 f4 67 00 00   ··.·
0030  00 00 78 09 08 00 00 00  00 00 10 11 12 13 14 15   ····
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ····
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()
0060  36 37                                              67
```

wireshark_enp0s1VLVL42.pcapng | Packets: 504 · Displayed: 34 (6.7%) · Dropped: 0 (0.0%) | Profile: Default