Project Requirement

The project requires demonstrating port scanning using multiple Nmap techniques including TCP, UDP, and service scanning with proper scan configurations documented. Service enumeration must be performed on identified services with detailed output analysis. Vulnerability scanning using Nessus Essentials will be executed with proper scope and configuration. All findings must be documented with evidence including scan configurations, raw output, and analysis of results. Documentation must include false positive analysis and verification steps.

Nmap Scanning Techniques

1. TCP SYN Scan

Command Used:
sudo nmap -sS -p- -v localhost

Explanation:

- `-sS`: Initiates a SYN (Stealth) scan, which is faster and less detectable.
- `-p-`: Scans all 65535 ports.
- `-v`: Enables verbose output for detailed information.
- `localhost`: The target system (127.0.0.1).

Scan Results:

- **Open Port:** 8834/tcp
- **Service:** `nessus-xmlrpc`

Analysis:

The open port 8834 is associated with Nessus, a well-known vulnerability scanner. The presence of this service indicates that the Nessus web interface or API might be accessible, which could be a security consideration if exposed to untrusted networks.

```
sh-3.2# nmap -sS -p- -v  localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 16:07 EST
Initiating SYN Stealth Scan at 16:07
Scanning localhost (127.0.0.1) [65535 ports]
Discovered open port 8834/tcp on 127.0.0.1
Completed SYN Stealth Scan at 16:07, 3.92s elapsed (65535 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE
8834/tcp open  nessus-xmlrpc

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.06 seconds
           Raw packets sent: 65535 (2.884MB) | Rcvd: 131071 (5.505MB)
```

---

2. UDP Scan

Command Used:
sudo nmap -sU -p- -v localhost

Explanation:

- `-sU`: Initiates a UDP scan to identify open UDP ports.
- `-p-`: Scans all available UDP ports (1-65535).
- `-v`: Verbose mode to get detailed output.

Scan Results:

- **Open/Filtered Ports:**
  - `137/udp` - netbios-ns
  - `138/udp` - netbios-dgm
  - `5353/udp` - zeroconf
  - Multiple high-range ports (e.g., 56005, 58596, 62813, 63118) showed as `open|filtered` with unknown services.

Analysis:

The `open|filtered` state indicates that Nmap cannot definitively determine if the port is open. This often occurs when no response is received. The presence of NetBIOS services (`137` and

138) could suggest a Windows environment or networked file sharing. The 5353/udp port is used by the mDNS (Multicast DNS), often for local network service discovery.

```
sh-3.2# nmap -sU -p- -v  localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 16:13 EST
Initiating UDP Scan at 16:13
Scanning localhost (127.0.0.1) [65535 ports]
Completed UDP Scan at 16:13, 6.83s elapsed (65535 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00089s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65528 closed udp ports (port-unreach)
PORT      STATE         SERVICE
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
5353/udp  open|filtered zeroconf
56005/udp open|filtered unknown
58596/udp open|filtered unknown
62813/udp open|filtered unknown
63118/udp open|filtered unknown

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.97 seconds
         _  Raw packets sent: 65641 (3.171MB) | Rcvd: 131260 (6.846MB)
```

3. Service Version Detection

Command Used:
sudo nmap -sV -p- -v localhost

Explanation:

- `-sV`: Enables version detection, which probes services to determine software versions.
- `-p-`: Scans all TCP ports.

Scan Results:

- **Open Port:** `8834/tcp`
- **Service:** `ssl/nessus-xmlrpc`
- **Version:** The service version could not be fully identified by Nmap, suggesting a custom or less common implementation of the `nessus-xmlrpc` service.

Analysis:

Since the service returned an unrecognized response, it could either be a custom service or a less common version of Nessus. This might require manual verification or using specialized Nessus plugins for further analysis.

```
sh-3.2# nmap -sV -p- -v localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 16:24 EST
NSE: Loaded 47 scripts for scanning.
Initiating SYN Stealth Scan at 16:24
Scanning localhost (127.0.0.1) [65535 ports]
Discovered open port 8834/tcp on 127.0.0.1
Completed SYN Stealth Scan at 16:24, 4.39s elapsed (65535 total ports)
Initiating Service scan at 16:24
Scanning 1 service on localhost (127.0.0.1)
Completed Service scan at 16:26, 137.95s elapsed (1 service on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 16:26
Completed NSE at 16:26, 0.03s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 1.02s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
8834/tcp open  ssl/nessus-xmlrpc?
1 service unrecognized despite returning data. If you know the service/version, please submit the
 following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8834-TCP:V=7.95%T=SSL%I=7%D=2/24%Time=67BCE3A4%P=x86_64-apple-darwi
SF:n21.6.0%r(HTTPOptions,81,"HTTP/1\.1\x20405\x20Method\x20not\x20Allowed\
SF:r\nConnection:\x20close\r\nDate:\x20Mon,\x2024\x20Feb\x202025\x2021:24:
SF:52\x20GMT\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\n\r\n")%r(R
SF:TSPRequest,7A,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clo
SF:se\r\nDate:\x20Mon,\x2024\x20Feb\x202025\x2021:24:52\x20GMT\r\nContent-
SF:Length:\x200\r\nServer:\x20NessusWWW\r\n\r\n")%r(Help,7A,"HTTP/1\.1\x20
SF:400\x20Bad\x20Request\r\nConnection:\x20close\r\nDate:\x20Mon,\x2024\x2
SF:0Feb\x202025\x2021:25:07\x20GMT\r\nContent-Length:\x200\r\nServer:\x20N
SF:essusWWW\r\n\r\n")%r(TerminalServerCookie,7A,"HTTP/1\.1\x20400\x20Bad\x
SF:20Request\r\nConnection:\x20close\r\nDate:\x20Mon,\x2024\x20Feb\x202025
SF:\x2021:25:12\x20GMT\r\nContent-Length:\x200\r\nServer:\x20NessusWWW\r\n
SF:\r\n")%r(SIPOptions,7A,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnectio
SF:n:\x20close\r\nDate:\x20Mon,\x2024\x20Feb\x202025\x2021:25:47\x20GMT\r\
SF:nContent-Length:\x200\r\nServer:\x20NessusWWW\r\n\r\n");

Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.02 seconds
        _  Raw packets sent: 65535 (2.884MB) | Rcvd: 131071 (5.505MB)
```

False Positive Analysis and Verification Steps

Identifying False Positives:

The `open|filtered` state on UDP ports could potentially be a false positive, especially if firewall rules drop packets without a response. Verification steps include:

- Using `nc -u <target_ip> <port>` to manually test UDP port response.

- Cross-verifying with another tool like `hping3` or `ncat`.

Verification Example:

nc -u 127.0.0.1 137

If no response is received, it is likely that the port is filtered rather than open.

Conclusion

The Nmap scanning portion of this project successfully identified open TCP and UDP ports and performed service enumeration. The next steps involve executing a Nessus Essentials vulnerability scan and integrating those results with the findings from Nmap. Detailed documentation of all scans and their outputs ensures a thorough analysis and provides a solid foundation for identifying potential security risks.