Task 1

Perform a Vulnerability Assessment of a Sample Web Application

Vulnerability Assessment Report : -

Tool Used : Nmap

- **Nmap (Network Mapper)** : Is an open-source tool used for network discovery and security auditing. It is primarily used to :-
- **Discover Hosts and Services**: Nmap identifies devices (hosts) on a network and determines which services (e.g., HTTP, FTP) are running on them.
- **Detect Operating Systems**: Nmap can attempt to detect the operating system (OS) running on remote devices.
- **Security Auditing**: Nmap helps in identifying potential vulnerabilities and misconfigurations in network devices and services.

---

1. Introduction : -

- **Objective**: -
- The purpose of this assessment is to identify potential security vulnerabilities within the target web application - **OWASP Juice Shop.**
- The assessment was conducted using **Nmap**, and this report provides a summary of the **identified vulnerabilities, their associated risks, and recommendations to mitigate them.**

---

2. Scope of the Assessment :-

The assessment was limited to the local network, targeting OWASP Juice Shop running on localhost and the associated ports. The primary objective was to detect:

- **Open ports and their associated services**
- **Potential misconfigurations or vulnerabilities in services**
- **OS and service details**

---

3. Findings :-

Open Ports and Services :-

The following open ports and associated services were identified :

Port	Service	Version	State	Notes
39459/TCP	**HTTP**	**Golang net/http**	**Open**	**Web server running on Golang (HTTP service)**
3000/TCP	**HTTP**	**(No specific service info)**	**Open**	**Likely OWASP Juice Shop web application on port 3000**

4. Vulnerabilities Description : -

□ **Port 39459/ TCP:**

- **Service:** Golang net/http server
- **State:** Open
- **Details:** This is an HTTP service running on a non-standard port (39459). The service returns 404 Not Found and 400 Bad Request responses when specific HTTP requests are made, indicating that the server might be a misconfigured or unused service.

□ **Port 3000/ TCP:**

- **Service:** HTTP (likely OWASP Juice Shop)
- **State:** Open
- **Details:** The default port for the OWASP Juice Shop application, commonly used for HTTP services.

□ 4.2 Service Misconfiguration and Risks Identified :-

□ **Unnecessary Open Golang HTTP Service (Port 39459/TCP)**

- **Risk:** The presence of an open HTTP service on port 39459 (Golang net/HTTP) is concerning. This service seems to be misconfigured or not in use, as it returns 404 Not Found or 400 Bad Request responses. Attackers could potentially leverage it if left unmonitored, as it could be used for further attacks like a denial of service (DoS) or information gathering.
- **Recommendation**:
    - ○ Disable or remove the service on port 39459 if it is unnecessary.

    - If the service is required, ensure it is properly configured, secure, and does not expose any sensitive information.
    - Monitor service behavior regularly to ensure it doesn't cause unexpected issues.

□ **Exposure of OWASP Juice Shop on Port 3000**

- **Risk**: The OWASP Juice Shop web application running on port 3000 may be vulnerable to several OWASP Top 10 vulnerabilities (e.g., SQL Injection, Cross-Site Scripting (XSS), etc.). As Juice Shop is designed to be insecure for testing purposes, it is crucial to assess the application's own security measures.
- **Recommendation**:
    - Conduct a web application security assessment (e.g., using OWASP ZAP or Burp Suite) to identify vulnerabilities such as SQL injection, XSS, and others.
    - Ensure proper input validation and sanitization are applied in the application to prevent injection attacks.
    - Apply security patches to the Juice Shop application and other web services it integrates with.

□ **Lack of Service Information and Detection for Port 3000**

- **Risk**: The service running on port 3000 did not return specific service information in the Nmap scan. While this is often a tactic to reduce information leakage, it can also indicate a potential misconfiguration that prevents proper identification of the service.
- **Recommendation**:
    - Ensure that the service on port 3000 is properly configured and its responses are appropriate for security auditing.
    - Limit information disclosure in HTTP headers to avoid giving attackers unnecessary details that could be exploited (e.g., application server details, version numbers).

□ **Insecure HTTP Service on Port 3000**

- Risk: The service on port 3000 is accessible without encryption (HTTP instead of HTTPS), which means data could be intercepted in transit by an attacker. This exposes sensitive data such as login credentials to man-in-the-middle (MITM) attacks.
- Recommendation:
    - Implement HTTPS to encrypt communication between the client and the server.
    - Obtain and configure a valid SSL/TLS certificate for the server to secure web traffic and prevent interception.

---

5. Conclusion : -

The vulnerability scan conducted using **Nmap** uncovered several risks, including unnecessary services, the use of HTTP without encryption, and potential misconfigurations in the OWASP Juice Shop application.

Key Recommendations to Mitigate Identified Risks :-

1. **Disable unused services**, particularly the Golang net/http server on port 39459.
2. **Secure the OWASP Juice Shop application** with HTTPS, ensuring encrypted communication.
3. **Regularly perform web application testing** to identify and mitigate security vulnerabilities.
4. **Monitor and manage services** to ensure they do not leak unnecessary information or expose risks.
5. **Apply security patches** to services and applications to reduce the attack surface.

6. Screenshots : -

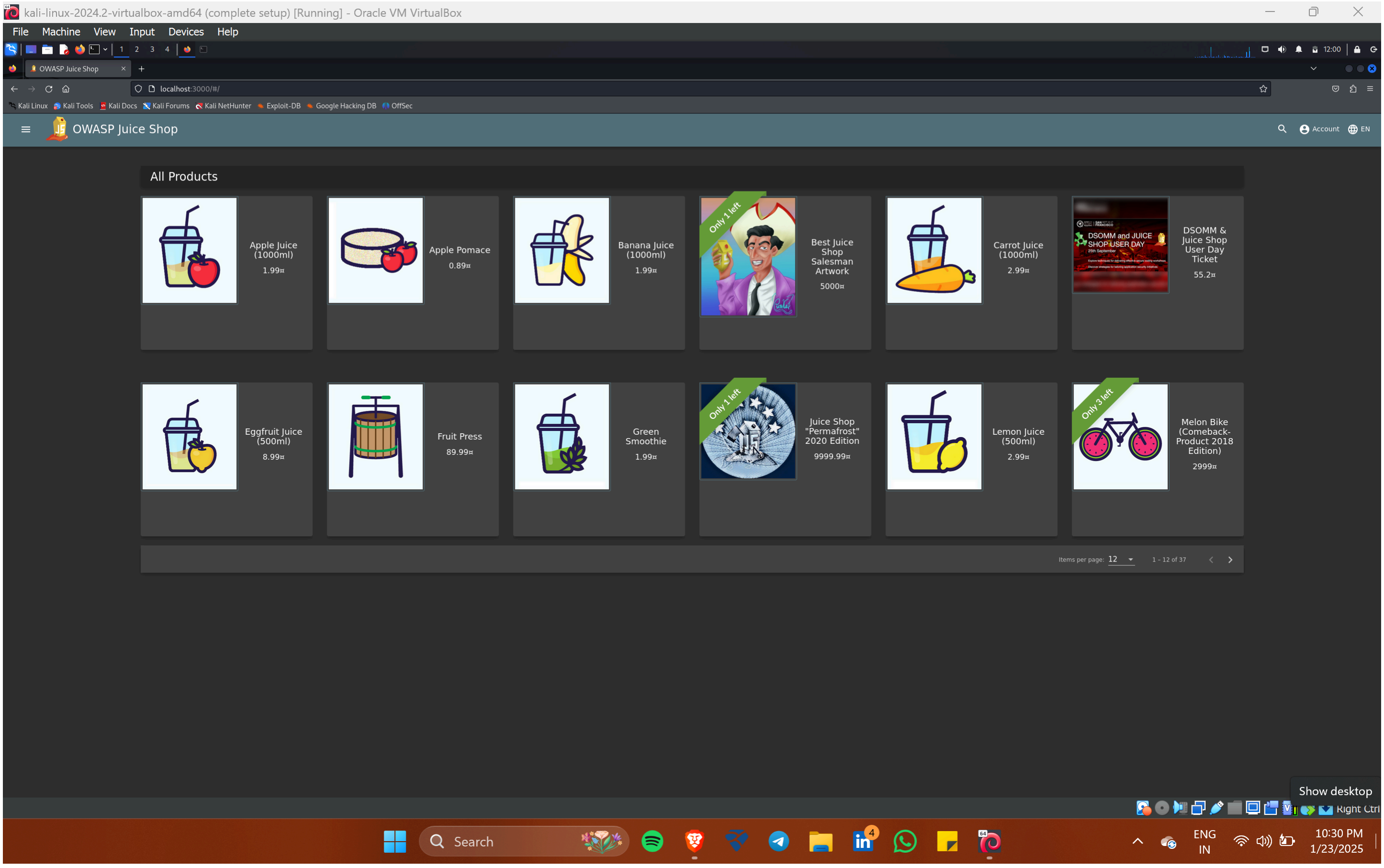
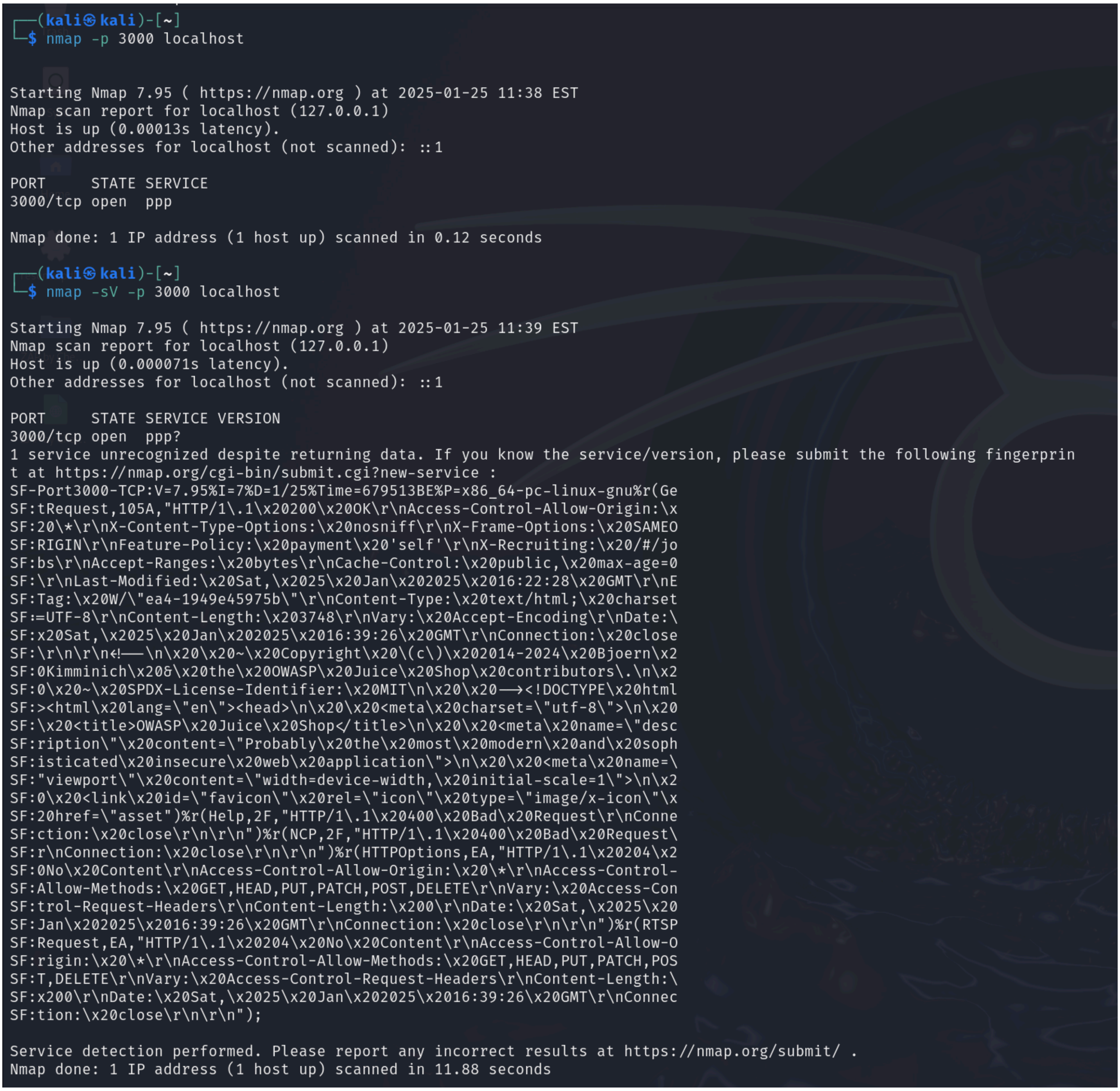
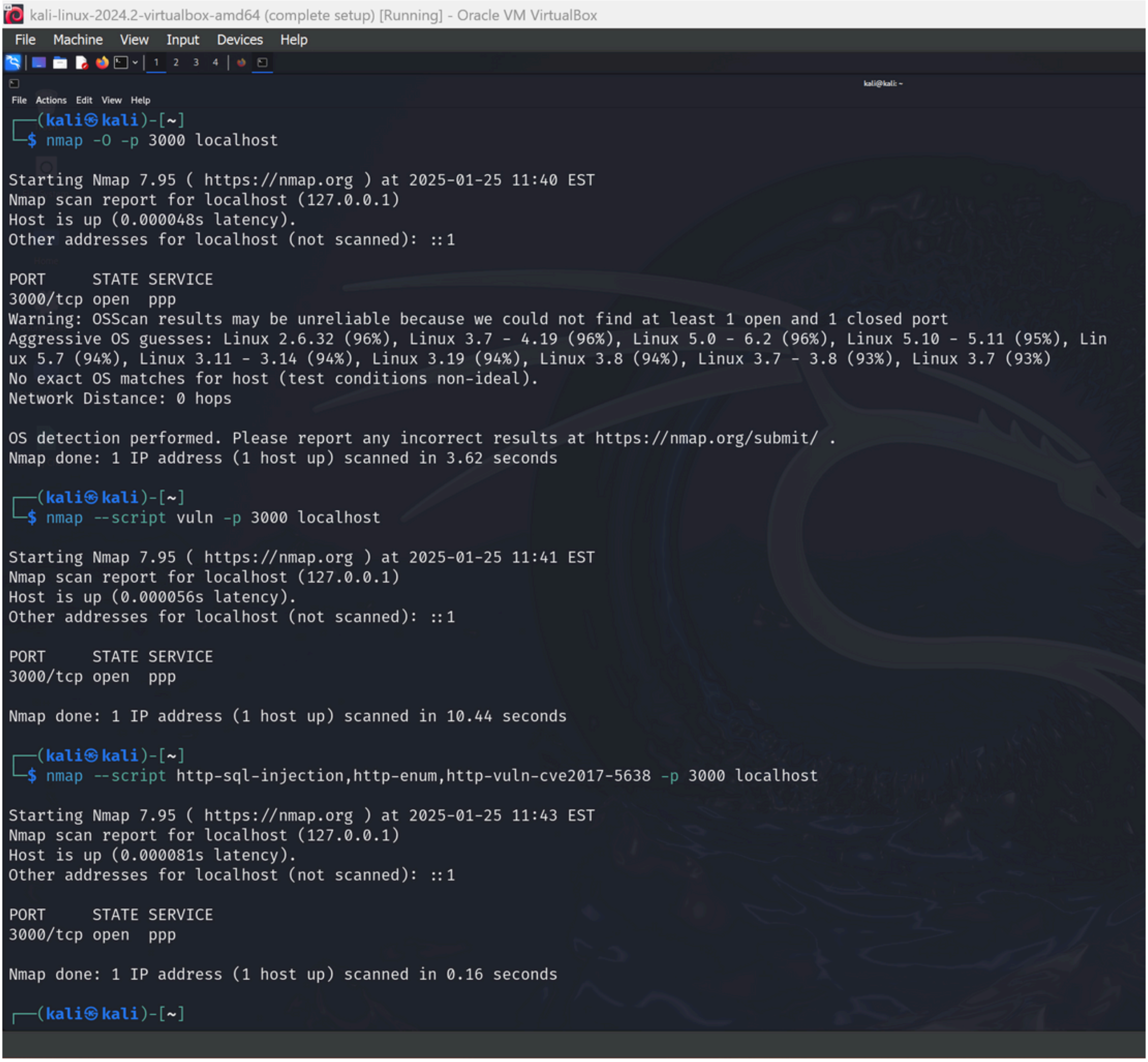

kali-linux-2024.2-virtualbox-amd64 (complete setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP Juice Shop
localhost:3000/#/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
Only 1 left
Best Juice Shop Salesman Artwork 5000¤
Carrot Juice (1000ml) 2.99¤
DSOMM and JUICE SHOP USER DAY
DSOMM & Juice Shop User Day Ticket 55.2¤
Eggfruit Juice (500ml) 8.99¤
Fruit Press 89.99¤
Green Smoothie 1.99¤
Only 1 left
Juice Shop "Permafrost" 2020 Edition 9999.99¤
Lemon Juice (500ml) 2.99¤
Only 3 left
Melon Bike (Comeback-Product 2018 Edition) 2999¤
Items per page: 12
1 - 12 of 37
Show desktop
Right Ctrl
Search
ENG IN
10:30 PM 1/23/2025

Figure - 1 : OWASP JUICE SHOP



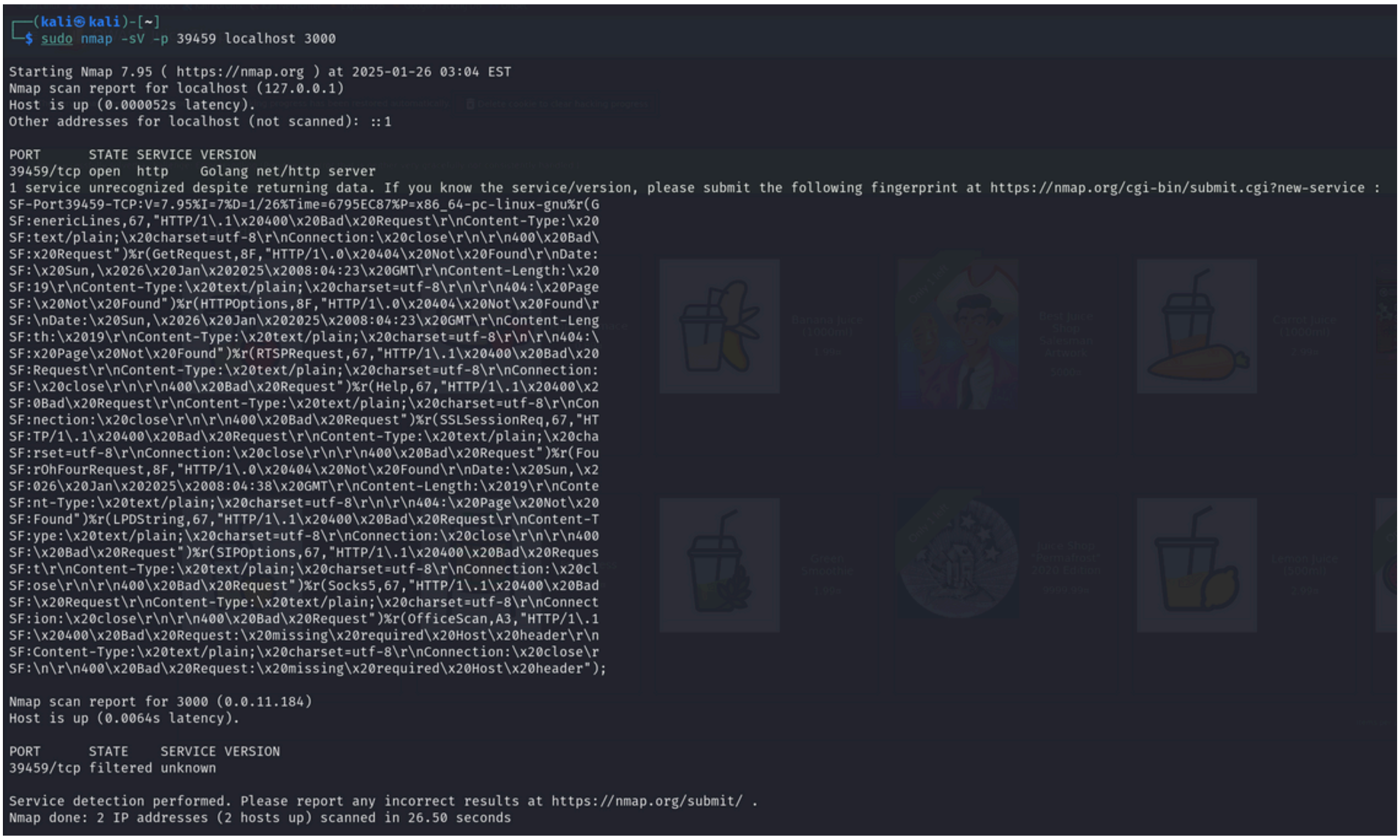
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3000 localhost


Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 11:38 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 3000 localhost

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 11:39 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
3000/tcp open  ppp?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprin
t at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.95%I=7%D=1/25%Time=679513BE%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,105A,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin:\x
SF:20\*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SAMEO
SF:RIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#/jo
SF:bs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=0
SF:\r\nLast-Modified:\x20Sat,\x2025\x20Jan\x202025\x2016:22:28\x20GMT\r\nE
SF:Tag:\x20W/\"ea4-1949e45975b\"\r\nContent-Type:\x20text/html;\x20charset
SF:=UTF-8\r\nContent-Length:\x203748\r\nVary:\x20Accept-Encoding\r\nDate:\
SF:x20Sat,\x2025\x20Jan\x202025\x2016:39:26\x20GMT\r\nConnection:\x20close
SF:\r\n\r\n<!--\n\x20\x20~\x20Copyright\x20\(c\)\x202014-2024\x20Bjoern\x2
SF:0Kimminich\x20&\x20the\x20OWASP\x20Juice\x20Shop\x20contributors\.\n\x2
SF:0\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20--><!DOCTYPE\x20html
SF:><html\x20lang=\"en\"><head>\n\x20\x20<meta\x20charset=\"utf-8\">\n\x20
SF:\x20<title>OWASP\x20Juice\x20Shop</title>\n\x20\x20<meta\x20name=\"desc
SF:ription\"\x20content=\"Probably\x20the\x20most\x20modern\x20and\x20soph
SF:isticated\x20insecure\x20web\x20application\">\n\x20\x20<meta\x20name=\
SF:"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n\x2
SF:0\x20<link\x20id=\"favicon\"\x20rel=\"icon\"\x20type=\"image/x-icon\"\x
SF:20href=\"asset")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConne
SF:ction:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x20204\x2
SF:0No\x20Content\r\nAccess-Control-Allow-Origin:\x20\*\r\nAccess-Control-
SF:Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-Con
SF:trol-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Sat,\x2025\x20
SF:Jan\x202025\x2016:39:26\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSP
SF:Request,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Allow-O
SF:rigin:\x20\*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POS
SF:T,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Length:\
SF:x200\r\nDate:\x20Sat,\x2025\x20Jan\x202025\x2016:39:26\x20GMT\r\nConnec
SF:tion:\x20close\r\n\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```

Figure - 2 : Basic Nmap scan and Service Version Detection Scan


kali-linux-2024.2-virtualbox-amd64 (complete setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -O -p 3000 localhost

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 11:40 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000048s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
3000/tcp open  ppp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.7 - 4.19 (96%), Linux 5.0 - 6.2 (96%), Linux 5.10 - 5.11 (95%), Lin
ux 5.7 (94%), Linux 3.11 - 3.14 (94%), Linux 3.19 (94%), Linux 3.8 (94%), Linux 3.7 - 3.8 (93%), Linux 3.7 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.62 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script vuln -p 3000 localhost

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 11:41 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 10.44 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script http-sql-injection,http-enum,http-vuln-cve2017-5638 -p 3000 localhost

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 11:43 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(kali㉿kali)-[~]
```

Figure - 3 : OS Detection vulnerability and web vulnerability Scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 39459 localhost 3000

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 03:04 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000052s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
39459/tcp open  http    Golang net/http server
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-Port39459-TCP:V=7.95%I=7%D=1/26%Time=6795EC87%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nDate:
SF:\x20Sun,\x2026\x20Jan\x202025\x2008:04:23\x20GMT\r\nContent-Length:\x20
SF:19\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\x20Page
SF:\x20Not\x20Found")%r(HTTPOptions,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r
SF:\nDate:\x20Sun,\x2026\x20Jan\x202025\x2008:04:23\x20GMT\r\nContent-Leng
SF:th:\x2019\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\
SF:x20Page\x20Not\x20Found")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nCon
SF:nection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Fou
SF:rOhFourRequest,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nDate:\x20Sun,\x2
SF:026\x20Jan\x202025\x2008:04:38\x20GMT\r\nContent-Length:\x2019\r\nConte
SF:nt-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\x20Page\x20Not\x20
SF:Found")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20cl
SF:ose\r\n\r\n400\x20Bad\x20Request")%r(Socks5,67,"HTTP/1\.1\x20400\x20Bad
SF:\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnect
SF:ion:\x20close\r\n\r\n400\x20Bad\x20Request")%r(OfficeScan,A3,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request:\x20missing\x20required\x20Host\x20header\r\n
SF:Content-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r
SF:\n\r\n400\x20Bad\x20Request:\x20missing\x20required\x20Host\x20header");

Nmap scan report for 3000 (0.0.11.184)
Host is up (0.0064s latency).

PORT      STATE    SERVICE VERSION
39459/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 26.50 seconds
```

Figure - 4 : Service Version Detection on Unknown Port 39459