

## **1. Introduction**

This report presents the Vulnerability Assessment performed as part of the Cybersecurity Internship. The objective was to identify open ports, running services, and operating system details of the target system using Nmap scanning techniques.

The assessment was conducted in a controlled environment using Kali Linux.

---

## **2. Objective**

- Identify open ports on the system
  - Detect running services
  - Perform OS detection
  - Analyze possible exposure
- 

## **3. Tools Used**

- Kali Linux
  - Nmap
- 

## **4. Commands Used**

### **Service Version Detection**

```
nmap -sV 127.0.0.1
```

### **OS Detection**

```
nmap -O 127.0.0.1
```

---

## **5. Findings**

The Nmap scan identified open ports and active services running on the system. Service detection helped in identifying the versions of services, which is important for vulnerability analysis.

OS detection revealed system information, which may help attackers if not properly secured.

---

## **6. Risk Analysis**

- Open ports increase attack surface
  - Unnecessary services can be exploited
  - Service version disclosure may expose known vulnerabilities
- 

## **7. Conclusion**

The vulnerability assessment successfully identified open ports and service information of the target system. This task helped in understanding reconnaissance and scanning techniques used in cybersecurity.