

Cybersecurity Internship Tasks

Name: Safiullah Shahid

Assignment: Task # 1

Position: Cyber Security Intern

Department: Cyber Security

Date of Submission: July 7, 2024

Company: Digital Empowerment

Network Penetration testing

For this task I will use a lab environment created in a VMWare Work Station. For this task I used the following systems

S/No	Systems	IP's
1.	Kali Linux (Our Pen testing Machine)	192.168.67.133
Target Systems		
2.	Windows 10	192.168.67.131
3.	OWASP Broken Web Apps	192.168.67.128
4.	Metasploitable Linux	192.168.67.132

IP's Found

- | | |
|-------------------|---------------------|
| 1. 192.168.67.1 | Possibly Router IP |
| 2. 192.168.67.2 | Possibly Gateway IP |
| 3. 192.168.67.133 | Our Machine IP |
| 4. 192.168.67.254 | Blocking IP |
| 5. 192.168.67.128 | |
| 6. 192.168.67.131 | |
| 7. 192.168.67.132 | |

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE -PS22,80,443 192.168.67.0/24 -oG - | awk '/Up$/ {print $2}'
[sudo] password for kali:
192.168.67.1    connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:
192.168.67.2    extension pgcrypto
192.168.67.128  connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:
192.168.67.131  connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:
192.168.67.132
192.168.67.254  extension pg-pgm
192.168.67.133  connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: FATAL:
```

