| Team #14 |
| --- |
|  |

# Memorandum

To: Management

From: Team #14

Date: February 18, 2023

Subject: Internal Services Evaluation

We have completed an assessment of the network services that are being offered on each internal server using a software tool called Nmap. Nmap is an open source utility used for network discovery and security auditing

With the Nmap scan complete, we have discovered the following network services that are being offered on each internal server, as outlined in the table below. For each server, I have listed the host name, host IP address, the protocol, port number, and the application description.

Sincerely,  
Team 14

Here are the results of the assessment:

| **Host Name** | **Host IP Address** | **Protocol/ Port Number** | **Application Description** | **Assessment** |
| --- | --- | --- | --- | --- |
| **2016 Docker/ Remote** | **Local IP: 172.20.240.10  Public IP: 172.25.20.34.97** | **N/A** | **N/A** | **N/A** |
| **Debian 8.5 DNS/NTP** | **Local IP: 172.20.240.20**  **Public IP: 172.25.20.34.20** | **UDP/123 (Expected)** | **NTP Server** | **No remediation needed** |
|  |  | **UDP/53 (Expected)** | **DNS Server** | **No remediation needed** |
|  |  | **UDP/953 (Expected)** | **DNS Server** | **No remediation needed** |
| **Ubuntu 14 Web** | **Local IP: 172.20.242.10**  **Public IP: 172.25.20.34.23** | **N/A** | **N/A** | **N/A** |
| **2012 AD/DNS/DHCP** | **Local IP: 172.20.242.200**  **Public IP: 172.25.20.34.27** | **UDP/123 (Expected?)** | **NTP Server?** | **No remediation needed** |
|  |  | **TCP/389 (Expected)** | **AD Server** | **No remediation needed** |
|  |  | **UDP/67 (Expected)** | **DHCP Server** | **No remediation needed** |
|  |  | **UDP/53 (Expected)** | **DNS Server** | **No remediation needed** |
|  |  | **TCP/3268 (Expected)** | **AD Server** | **No remediation needed** |
| **Ubuntu Wkst** | **DHCP** | **N/A** | **N/A** | **N/A** |
| **Splunk** | **Local IP: 172.20.241.20**  **Public IP: 172.25.20.34.9** | **TCP/8000 (Expected)** | **Web interface for Splunk** | **No remediation needed** |
|  |  | **TCP/8089 (Expected)** | **Splunk Server** | **No remediation needed** |
|  |  | **TCP/9997** | **Splunk Server** | **No remediation needed** |
|  |  | **TCP/8065 (Expected)** | **Splunk Server** | **No remediation needed** |
| **CentOS 7 E-comm** | **Local IP: 172.20.241.30**  **Public IP: 172.25.20.34.11** | **TCP/80 (Expected)** | **Web Server** | **No remediation needed** |
|  |  | **TCP/3306 (Expected)** | **MySQL Server** | **No remediation needed** |
| **Fedora 21 Webmail/ WebApps** | **Local IP: 172.20.241.40**  **Public IP: 172.25.20.34.39** | **TCP/110 (Expected)** | **Email Server** | **No remediation needed** |
|  |  | **TCP/25 (Expected)** | **Email Server** | **No remediation needed** |
|  |  | **TCP/143 (Expected)** | **Email Server** | **No remediation needed** |