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

# Memorandum

To: Management

From: Team #14

Date: February 18, 2023

Subject: Inventory Report

We have provided an updated inventory report of all the network devices in our infrastructure, including important information such as IP addresses, current and available OS levels, vulnerabilities, and upgrade recommendations.

Attached is a table that catalogs each network device and includes the following information for each device:

* Device Name and Function
* Device IP address
* Device MAC address
* OS Level currently installed
* Known vulnerabilities
* Upgrade recommendation

Please take a moment to review the attached table. If you have any questions or concerns regarding the upgrade recommendations, don't hesitate to reach out.

Sincerely,

Team 14

| **Device Name/ Function** | **Device IP Address(es)** | **Device MAC Address** | **O/S Level Currently Installed** | **Vulnerabilities** | **Upgrades Needed** |
| --- | --- | --- | --- | --- | --- |
| **Windows 10 (Client)** | **172.31.34.5** | **00:50:56:9E:17:46** | **Windows 10** | **Privilege Escalation (CVE-2022-37969)**  **RCE (CVE-2022-34722)** | **Upgrade to Windows 11** |
| **2016 Docker/ Remote (Server)** | **Local IP: 172.20.240.10  Public IP: 172.25.20.34.97** | **00:15:5D:FE:2A:A0** | **Windows Server 2016 Standard** | **Hyper-V RCE (CVE-2021-34450)**  **Eternal Blue (CVE-2017-0144)** | **Upgrade to Windows Server 2022** |
| **Debian 8.5 DNS/NTP (Server)** | **Local IP: 172.20.240.20**  **Public IP: 172.25.20.34.20** | **00:50:56:9E:5A:07** | **Debian 8.5** | **Privilege Escalation (CVE-2016-5696)**  **RCE (CVE-2011-1930)** | **Upgrade to Debian 11** |
| **Ubuntu 14 Web (Server)** | **Local IP: 172.20.242.10**  **Public IP: 172.25.20.34.23** | **00:50:56:9E:94:28** | **Ubuntu 14.04.2** | **RCE (CVE-2011-2767)**  **DOS (CVE-2014-1528)** | **Upgrade to Ubuntu 22.04** |
| **2012 AD/DNS/ DHCP (Server)** | **Local IP: 172.20.242.200**  **Public IP: 172.25.20.34.27** | **00:50:56:9E:9E:48** | **Windows Server 2012 Standard** | **Print Spooler Privilege Escalation (CVE-2023-21760)**  **RCE (CVE-2022-44667)** | **Upgrade to Windows Server 2022** |
| **Ubuntu Wkst (Client)** | **DHCP** | **00:50:56:9E:75:D6** | **Ubuntu Desktop 12.04** | **Error Handling (CVE-2020-8625)**  **Privilege Escalation (CVE-2013-2094)** | **Upgrade to Ubuntu Desktop 22.10** |
| **Splunk (Server)** | **Local IP: 172.20.241.20**  **Public IP: 172.25.20.34.9** | **00:50:56:9D:75:2D** | **CentOS 7** | **Privilege Escalation (CVE-2020-5291)**  **RCE (CVE-2017-7477)** | **CentOS is at EOL** |
| **CentOS 7 E-comm (Server)** | **Local IP: 172.20.241.30**  **Public IP: 172.25.20.34.11** | **00:50:56:9E:72:EA** | **CentOS 7** | **Privilege Escalation (CVE-2020-5291)  RCE (CVE-2017-7477)** | **CentOS is at EOL** |
| **Fedora 21 Webmail/ WebApps (Server)** | **Local IP: 172.20.241.40**  **Public IP: 172.25.20.34.39** | **00:50:56:9E:91:10** | **Fedora 21** | **Privilege Escalation (CVE-2015-0278)**  **Buffer Overflow (CVE-2015-2806)** | **Upgrade to Fedora 37** |
| **Palo Alto (Firewall)** | **172.20.242.150** | **7C:89:C2:99:12:10** | **PAN OS 10.0.0** | **RCE (CVE-2022-0024)**  **RCE (CVE-2021-3061)** | **Upgrade to PAN OS 11.0.0** |