**MEMORANDUM**

To: Management

From: Team

Subject: Evaluate External Perimeter for Risk Vulnerabilities

Date:

The security team has completed an external perimeter scan of the organization’s network. This was accomplished by scanning all subnets with the network scanning tool known as Nmap. With Nmap, the security team identified open ports, exposed services, and service versions for the devices in the network. Service identification was completed using Nmap’s fingerprinting feature. The results are enumerated in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Port | Service | Version |
| 172.20.241.20 | 8000/tcp | http | Splunk httpd |
| 172.20.241.30 | 22/tcp | ssh | OpenSSH 6.6.1 |

Nmap’s service fingerprinting was unable to identify the service version of every open port from the perimeter. From the service versions that were identified, we ascertained that these servers are vulnerable to certain known exploits in a possible attack on the service.

**Vulnerabilities Discovered**

For the service \_\_\_, we found that the version \_\_\_ was vulnerable to exploits that \_\_\_ This vulnerability is identified under CVE-\_\_\_\_\_.

The images below show vulnerabilities found on the \_\_\_\_ machine which is within the organization’s current infrastructure. This specific vulnerability show is CVE-\_\_\_\_.

**Figure 1.** Server showing vulnerable version

Please let us know if there are any additional actions that should be performed at this time.

Thank you,

Team 01