Internal Memorandum

To: hal.cio@seccdc.org

CC: judge_29@seccdc.org

From: hal29@seccc.org

Date: Feburary 23rd 2019

Memo #: #19-P4

Re: System Vulnerability Scan

Hierarchical Access Limited Corporation

www.halcorp.biz

Hello,

As per your request, system vulnerability scans have been performed on our MySQL, Webmail, E-commerce & Active Directory/DNS servers. We used the scanning utility Nmap to conduct this scan. Below are the top 3 vulnerabilities that were found for each system:

AD/DNS:

1. Zone Transfers
    a. **Issue**: Zone transfers are currently allowed from all systems on the network, allowing anyone to replicate DNS databases.
    b. **Resolution**: The system administration team can restrict the zone transfers to only be allowed from other DNS servers on our network.
2. User Accounts with Simple Passwords
    a. **Issue:** Current user accounts on the local system have easy passwords that can be cracked.
    b. **Resolution:** This can be resolved by enforcing a strong password policy on the domain and having all corporate users change their current passwords.
3. Eternal Blue SMB Exploit
    a. **Issue**: The system is vulnerable to SMB exploit MS17_010, commonly known as Eternal Blue.
    b. **Resolution:** An update for this vulnerability can be applied through Windows Update or a specific patch for this exploit can be done.

Webmail:

1. Remote process access
    a. **Issue**: This version of Apache (2.4.16) is vulnerable to CVE-2017-9798. This vulnerability states that: “Apache httpd allows remote attackers to read secret data from process memory.”
    b. **Resolution**: The system administration team can update the apache service to a non-vulnerable version.
2. Unknown ssh keys
    a. **Issue:** Current user accounts on the local system have ssh keys that are unrecognized and don’t belong to our administration team.

This document is for the explicit purpose of supporting the 2018 SECCDC Preliminary Qualification Competition. Any similarity to organizations or persons real or imagined is purely coincidental. Do not disclose this document to anyone without the expressed permission of the competition organizers.

b. **Resolution:** This can be resolved by removing all unknown SSH keys and ensuring any future keys are audited.

3. Dovecot Denial of Service Vulnerability
    a. **Issue**: The system is vulnerable to Denial of Service vulnerability CVE-2017-15130. This exists in Dovecot before 2.2.34. An attacker may be able to cause excessive memory usage and force the process to restart.
    b. **Resolution:** An update for this vulnerability can be applied through a Dovecot update or a specific patch for this exploit can be done.

E-commerce:

1. PHP backdoor
    a. **Issue**: This site had a known php backdoor on the web server.
    b. **Resolution**: The system administration team can remove the backdoor from the system and audit any new php files.
2. Unknown ssh keys
    a. **Issue:** Current user accounts on the local system have ssh keys that are unrecognized and don't belong to our administration team.
    b. **Resolution:** This can be resolved by removing all unknown SSH keys and ensuring any future keys are audited.
3. Apache Denial of Service Vulnerability
    a. **Issue**: The system is vulnerable to Denial of Service vulnerability CVE-2011-3192. This exists in Apache before 2.2.9. This version of apache has a vulnerability that allows low privileged users to gain local administrator rights.
    b. **Resolution:** An update for this vulnerability can be applied through an Apache update or a specific patch for this exploit can be done.

MySQL:

1. Insecure mysql account
    a. **Issue:** Current MySQL accounts on the local system have easy passwords that can be cracked.
    b. **Resolution:** This can be resolved by enforcing a strong password policy and having all corporate users change their current passwords.
2. MySQL worldwide access
    a. **Issue:** Currently the MySQL database is open to the entire world. This is unnecessary for our business needs as the database simply needs to be open to our internal Linux services.
    b. **Resolution:** This can be resolved by removing all unknown SSH keys and ensuring any future keys are audited.
3. VNC Desktop enabled
    a. **Issue**: The system had a VNC server installed and enabled. That would allow a remote attacker to control the desktop of the system.
    b. **Resolution:** A fix for this would be to disable the VNC server and disable it at the firewall level.

Below is each of the nmap scans conducted:

This document is for the explicit purpose of supporting the 2018 SECCDC Preliminary Qualification Competition. Any similarity to organizations or persons real or imagined is purely coincidental. Do not disclose this document to anyone without the expressed permission of the competition organizers.

Debian Mysql machine:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2019-02-23 14:40 CST
Nmap scan report for thrat.frog.com (172.20.240.20)
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
root@fedora ~# _
```

Fedora webmail machine:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2019-02-23 14:40 CST
Nmap scan report for thrat.frog.com (172.20.240.20)
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
root@fedora ~# _
```

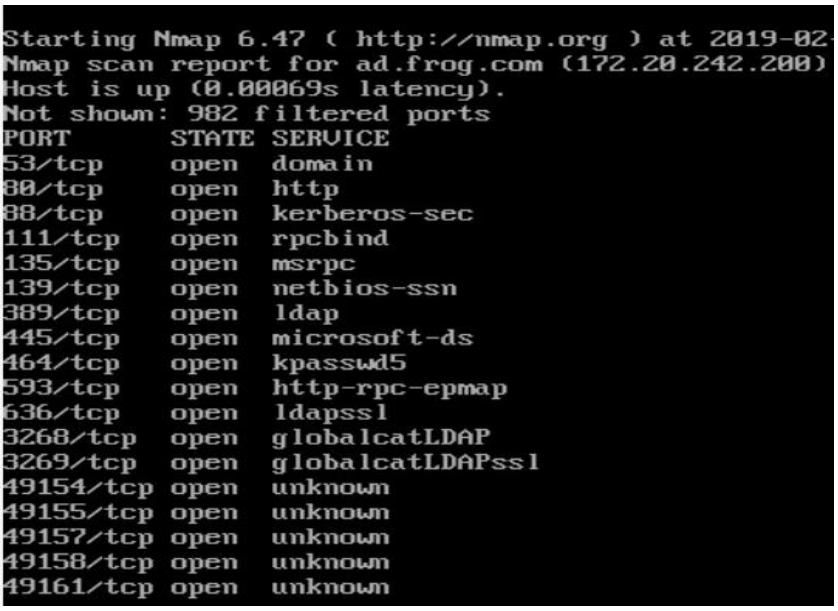
Centos Ecommerce machine:

```
root@fedora ~# nmap 172.20.241.30 -Pn

Starting Nmap 6.47 ( http://nmap.org ) at 2019-02-23 14:42 CST
Nmap scan report for 172.20.241.30
Host is up (0.00022s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:50:56:A4:98:36 (VMware)
```

This document is for the explicit purpose of supporting the 2018 SECCDC Preliminary Qualification Competition. Any similarity to organizations or persons real or imagined is purely coincidental. Do not disclose this document to anyone without the expressed permission of the competition organizers.

Acitive Directory/ DNS Machine



In accordance with HAL Memorandum policy, the entire header must be completed or the recipient may not acknowledge this as an official memorandum. Professional communications methods and decorum must be observed at all times.

This document is for the explicit purpose of supporting the 2018 SECCDC Preliminary Qualification Competition. Any similarity to organizations or persons real or imagined is purely coincidental. Do not disclose this document to anyone without the expressed permission of the competition organizers.