

Internal Memorandum

**To:** [hal.cio@seccdc.org](mailto:hal.cio@seccdc.org)

**CC:** [judge\_29@seccdc.org](mailto:judge_29@seccdc.org)

**From:** [hal29@seccc.org](mailto:hal29@seccc.org)

**Date:** March 31, 2019

**Memo #:** #07

**Re:** Security Audit

**Hello,**

As per your request, system vulnerability scans have been performed on our MySQL, Webmail, E-commerce, WWW, & 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
   1. **Issue**: Zone transfers are currently allowed from all systems on the network, allowing anyone to replicate DNS databases.
   2. **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
   1. **Issue:** Current user accounts on the local system have easy passwords that can be cracked.
   2. **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
   1. **Issue**: The system is vulnerable to SMB exploit MS17\_010, commonly known as Eternal Blue.
   2. **Resolution:** An update for this vulnerability can be applied through Windows Update or a specific patch for this exploit can be done.

WWW:

1. Unknown account

a. **Issue:** There existed accounts on the web server that were unknown and not created by the local branch IT team.

b. **Resolution:** Removed the accounts from the server and notified all other system owners. Will audit any future new accounts.

2. Directory browsing

a. **Issue:** The web server allowed directory browsing which would allow an attacker to browse the web folder and view all files in that directory.

b. **Resolution:** Can disable directory browsing within Internet information services and regularly check IIS settings.

3. Network level authentication

a. Issue: Allowed network level authentication on the remote desktop service. This vulnerability would allow insecure clients to connect to the machine.

b. Resolution: Can require network level authentication within remote desktop services and regularly check RDP settings.

Webmail:

1. Apache critical vulnerability
   1. **Issue**: This version of Apache (1.0) is vulnerable to CVE-2017-9798. This vulnerability states that: “Apache httpd allows remote attackers to read secret data from process memory.”
   2. **Resolution**: The system administration team can update the apache service to a non-vulnerable version.
2. Unknown ssh keys
   1. **Issue:** Current user accounts on the local system have ssh keys that are unrecognized and don’t belong to our administration team.
   2. **Resolution:** This can be resolved by removing all unknown SSH keys and ensuring any future keys are audited.
3. Dovecot Denial of Service Vulnerability
   1. **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.
   2. **Resolution:** An update for this vulnerability can be applied through a Dovecot update or a specific patch for this exploit can be done.

ECommerce:

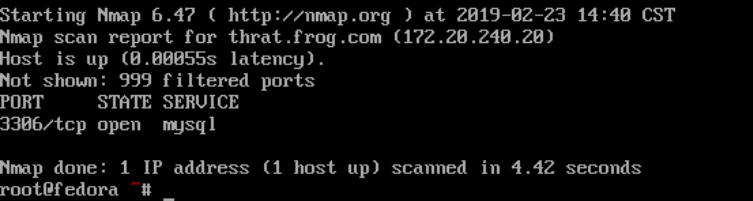
1. PHP backdoor
   1. **Issue**: This site had a known php backdoor on the web server.
   2. **Resolution**: The system administration team can remove the backdoor from the system and audit any new php files.
2. Malicious Cron jobs
   1. **Issue:** Currently the local system has cron jobs that are unrecognized and contain malicious actions that our administration team wouldn’t have setup.
   2. **Resolution:** This can be resolved by removing all unknown Cron jobs and ensuring any Cron jobs are audited.
3. Apache Denial of Service Vulnerability
   1. **Issue**: The system is vulnerable to Denial of Service vulnerabilities in old Apache versions. This exists in any outdated Apache version and can cause an outage in the web service of Apache version 2.2.14 (which we currently have installed).
   2. **Resolution:** An update for this vulnerability can be applied through an Apache update or a specific patch to this DOS vulnerability.

Database server:

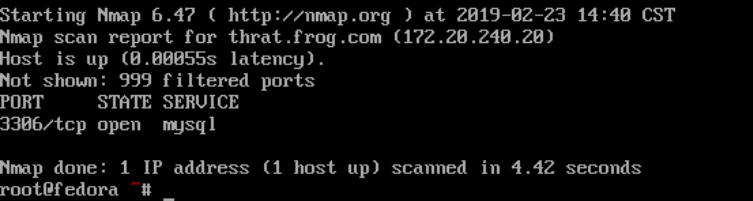
1. Insecure mysql account
   1. **Issue:** Current MySQL accounts on the local system have easy passwords that can be cracked.
   2. **Resolution:** This can be resolved by enforcing a strong password policy and having all corporate users change their current passwords.
2. MySQL worldwide access
   1. **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.
   2. **Resolution:** This can be resolved by removing all unknown SSH keys and ensuring any future keys are audited.
3. VNC Desktop enabled
   1. **Issue**: The system had a VNC server installed and enabled. That would allow a remote attacker to control the desktop of the system.
   2. **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:

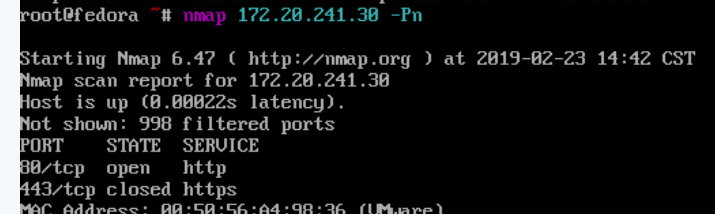
# Debian Mysql machine:



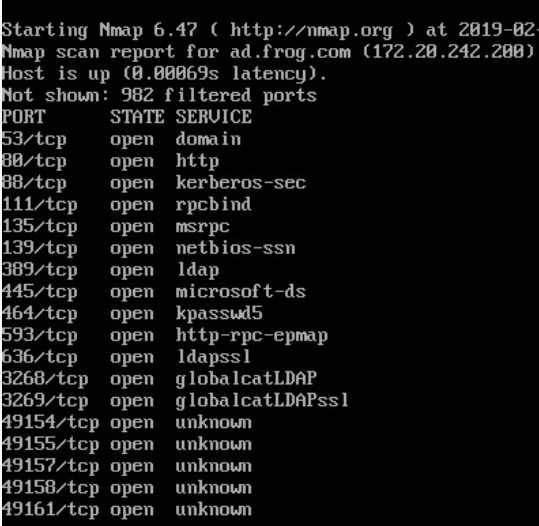
# Fedora webmail machine:



# Centos Ecommerce machine:



# 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.*