ProLUG – System Hardening

Required Materials

Putty

Rocky Server

Root or sudo command access

EXERCISES (Warmup to quickly run through your system and familiarize yourself)

1. ss -ntulp
    a. What ports are open on this server?
    b. What is open on port 9080?
        i. What does this service do?
2. systemctl --failed
    a. Are there any failed units?
3. systemctl list-units --state=active
    a. About how many active units are there?
        i. systemctl list-units --state=active | wc -l
4. rpm -qa | wc -l
    a. Approximately how many software packages do you have?
5. rpm -qa | grep -i ssh
    a. How many ssh packages do you have?
    b. What is the version of openssh?
        i. Do you know if there are any known vulnerabilities for that version?
            1. https://nvd.nist.gov/vuln/search

LAB

There will be three basic tasks for today's labs:

1. You will scan a server for a SCC Report and get a STIG Score

2. You will remediate some of the items from the scan

3. You will rescan and verify a better score.

SCC Report:

This lab portion can be done in the ProLUG Rocky servers, or in killercoda at this location:
https://killercoda.com/het-tanis/course/Linux-Labs/207-OS_STIG_Scan_with_SCC_Tool

1. Testing hardening on the ProLUG Lab may take over an hour. You are welcome to perform the test there, but make sure you have some time.

Ssh into a Rocky sever

cd /opt/scc

time ./cscc

---- Wait over an hour ------

cd /root/SCC/sessions #find the most recent run

Look in the results to see output.

Harden the system

1. Harden sshd

Red Hat Enterprise Linux 9 Security Technical Implementation Guide :: Version 2, Release: 1 Benchmark Date: 24 Jul 2024

Vul ID: V-258001 **Rule ID**: SV-258001r991589_rule **STIG ID**: RHEL-09-255125

Severity: CAT II **Classification**: Unclass

Group Title: SRG-OS-000480-GPOS-00227

Rule Title: RHEL 9 SSH public host key files must have mode 0644 or less permissive.

Discussion: If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Check Text: Verify the SSH public host key files have a mode of "0644" or less permissive with the following command:

Note: SSH public key files may be found in other directories on the system depending on the installation.

$ sudo stat -c "%a %n" /etc/ssh/*.pub

644 /etc/ssh/ssh_host_dsa_key.pub
644 /etc/ssh/ssh_host_ecdsa_key.pub
644 /etc/ssh/ssh_host_ed25519_key.pub
644 /etc/ssh/ssh_host_rsa_key.pub

If any key.pub file has a mode more permissive than "0644", this is a finding.

Fix Text: Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

$ sudo chmod 0644 /etc/ssh/*key.pub

Restart the SSH daemon for the changes to take effect:

$ sudo systemctl restart sshd.service

Is your system hardened in this capacity?

How did you check?

Did the fix check work for you?

How did you check?

2. Remove unneeded Software

Read about cowsay – man cowsay

Remove cowsay – dnf remove cowsay

```
[root@rocky1 ssh]# echo "This is terrible" | cowsay -p
 ____________________
< This is terrible >
 --------------------
        \   ^__^
         \  (@@)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
[root@rocky1 ssh]# echo "This is terrible" | cowsay -d
 ____________________
< This is terrible >
 --------------------
        \   ^__^
         \  (xx)\_______
            (__)\       )\/\
             U  ||----w |
                ||     ||
[root@rocky1 ssh]# echo "This is terrible" | cowsay -s
 ____________________
< This is terrible >
 --------------------
        \   ^__^
         \  (**)\_______
            (__)\       )\/\
             U  ||----w |
                ||     ||
```

Rescan to validate change

Ssh into a Rocky sever

cd /opt/scc

time ./cscc

---- Wait over an hour ------

cd /root/SCC/sessions #find the most recent run

Look in the results to see output.