

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: <u>https://killercoda.com/het-tanis/course/Linux-Labs/207-OS_STIG_Scan_with_SCC_Tool</u>



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 -----

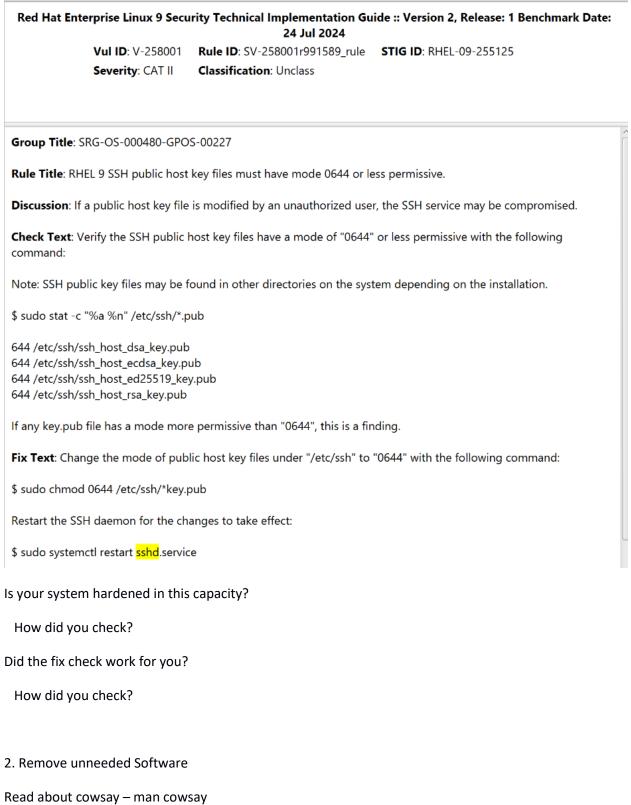
cd /root/SCC/sessions #find the most recent run

Look in the results to see output.

Harden the system

1. Harden sshd





Remove cowsay - dnf remove cowsay



[root@rocky1 ssh]# echo "This is terrible" | cowsay -p This is terrible > (00) \)\/\) \ | |----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 > (**) $) \setminus / \setminus$ 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.