Linux Hardening Guide

Kevin Schoonver, Gavin Lewis

January 8, 2021

Contents

Part I
SOP

1 Standard Operating Procedures

A Cyber Defense Competition is won by working together, working quickly, and working smartly to keep the dirty Red Team from keeping us down. Our goal is simple, keep the given services online and accessible. To achieve this goal we can imagine the competition as a game, with the pregame and game time. Pregame is everything up to the day of the competition, while the game is that nice long 8 hour period of being the nail for a very large hammer.

During the Pregame we typically have some information about the systems we will be using. Whether it's the services that are running on them, or the operating systems and their versions, any information is good information that can be used to make an attack plan.

The Game is everything else. The team has to use their prior knowledge and skills to lock down the system and make sure they stay up. They also have to be monitoring the systems for intrusions, and creating reports when anything fishy is found.

The goal of this document is to provide a set of procedures for most scenarios that would occur during the pregame and the game. There will be instructions on what needs to be done in each phase.

Test phrase

2 Pregame

In an ideal world, the Pregame would happen before the Game so we have time to view the environment before actually competing. When we cannot pregame, we must remove the CVE checks and most of the port scans until later in the competition after we have secured the network.

2.1 Assess

1. Run port scans
2. Write down all machines and their OS versions
3. Get process list from each machine
4. Check contents of \temp
   (a) Should be empty, make note of anything in here.
5. Check contents of \bin
   (a) Are there any files that look weird?

6. Check contents of home folders
7. Write down all users on the machine and what groups they are in
8. If there is time/is possible, download clamav and run it
    (a) This will alert us to files that have been tampered with
9. Check .bashrc for startup scripts or weird things

2.2 Research

1. Check OS versions on cvedetails.com
    (a) Make note of anything with a rating of 7 or higher
    (b) These may not all be useful, but some will
2. Do the same with software running on the machine
3. See if processes running on the machine should be there
    (a) ex) Apache probably should not be running on a DNS server
4. Make a list of ports that should be open on the machine
    (a) If it is a web server, then 80, 443, 53, 22 should be open at least, shut down the rest

2.3 Plan

1. Using all the gathered information, make a game pan for each machine that will happen during the first hour plan
2. Add programs/processes that should be stopped
3. Add files that should be deleted
4. List users that should be investigated

3 Game

This includes the first hour plan. After the first hour, operations will be cyclical and individual to each person and their machine.

3.1 First Hour

1. If we are allowed to, take a snapshot of the machine
2. Update the machine
   (a) This will indicate if the repos are fine. It is also good practive to check the repos to make sure they are legitimate
3. Create a new user and give it sudo access
4. Disable the root account
5. Check for other suspicious accounts and disable them
   (a) We disable instead of deleting just in case they need to be there
6. Check sudoers group for rogue users
7. Check for suspicious files in directories
8. Update the local firewall to what you need
9. Check for cron jobs
10. Implement the plan for this machine based on the Pregame
    (a) If there was no pregame, and there is still time in the first hour, do what should have been done in the pregame and gather as much info as you can.

3.2 Secure

Stop all intrusions

3.3 Fix

3.4 Monitor

Part II
Tools

4 Setup Up Package Repository

The majority of the linux boxes you will be faced with will not have the proper package repositories to collect packages. Whether it be a Debian, Ubuntu, or Fedora, if the version is no longer support by the maintainers of the distro, you will need to change the location in which the package manager will look for

repositories. The distro probably supports some sort of archive in which the packages are kept, but no longer updated.

Please view the sections below to update the package repositories on various systems.

4.1 Ubuntu

```
#!/bin/bash
cp /etc/apt/sources.list /etc/apt/sources.list.bak #
    Backup sources list
sudo sed -i -re "s/([a-z]{2}\.)?archive.ubuntu.com|
    security.ubuntu.com/old-releases.ubuntu.com/g" /etc
    /apt/sources.list
```

4.2 Debian

```
#!/bin/bash
cp /etc/apt/sources.list /etc/apt/sources.list.bak #
    Backup sources list
sed "s/^deb/#deb/g" -i /etc/apt/sources.list  #
    Comment old sources

cat << EOF >> /etc/apt/sources.list
deb http://archive.debian.org/debian/ <version> main
    non-free contrib
deb-src http://archive.debian.org/debian/ <version>
    main non-free contrib

deb http://archive.debian.org/debian-security/ <
    version>/updates main non-free contrib
deb-src http://archive.debian.org/debian-security/ <
    version>/updates main non-free contrib
EOF
```

4.3 CentOS

```
#!/bin/bash
cp /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/
    CentOS-Base.repo.bak # Backup sources
cp /etc/yum.repos.d/CentOS-Vault.repo /etc/yum.repos.d
    /CentOS-Base.repo # Overwrite with Vault
sed -i -re "s/enabled.=.1/enabled = 0/g" /etc/yum.
    repos.d/rpmforge.repo
```

```
sed -i -re "s/enabled.=.0/enabled = 1/g" /etc/yum.
    repos.d/CentOS-Base.repo
```

5 User Management

5.1 Check .bashrc

Check the local **.bashrc** to ensure that any rogue commands are not run. If there is anything malicious in the **.bashrc**, remove and then reboot the machine.

5.2 Change Administrator Passwords

Utilize the password format excel document to change the account of any high-priviledge accounts on the machine. As well as important system users such as the mysql account.

```
#!/bin/bash
passwd <user> # Exclude <user> for changing current
    account
```

5.3 Create New Administrator Account

Make a new administrator account which will be used for all future administrative tasks. Disable any other administrative accounts which can be used by the attackers to run commands as an elevated user.

```
#!/bin/bash
adduser # Creates a new user
usermod -a -G sudo USERNAME # Add user to sudo
su USERNAME # Change to the new uesr
sudo ls # Test that the sudo works
```

5.4 Check for suspicious accounts

Check the system groups to determine if certain suspicious accounts are in groups they should not be. To check all the groups, run the following command:

```
#!/bin/bash
cat /etc/group | sort | less
```

Be sure to check the normal administrative groups such as **sudo**, **wheel**, **admin**, and **root**. Make note of these suspicious accounts.

Next, check all of the users on the system using the following command:

```
#!/bin/bash
less /etc/passwd
```

The users in this file are listed in chronological order based on when they were added so users later in the list are more likely to be rogue accounts. For service accounts such as **avahi**, they SHOULD NOT have a login shell nor a home directory such as
avahi:x:107:114:Avahi mDNS daemon,,,:**/home/bob:/bin/bash**
Daemons like Avahi should have their shells set to **/bin/false**, **/sbin/nologin**, or **/usr/sbin/nologin**.

Lastly, check the **sudoers** file. This should only contain administrative accounts such as **root** or **admin**. Use the command:

```
#!/bin/bash
less /etc/sudoers
```

5.5 Disable / Update Administrator and System Accounts

Now that you have the new administrator account, you will no longer need any of the other administrative accounts such as **root** or **administrator**. To disable these accounts, use the following command:

```
#!/bin/bash
usermod --lock --shell /usr/sbin/nologin --expiredate
    1970-02-02 USERNAME
```

Look for system / services accounts which are used to run various services or applications.

5.6 Check Sudoers Group

There should only be a couple of accounts in this group, the one you created and the **root** or **administrator** account that came with the box.

6 Check for suspicious files

Follows are methods used to find suspicious files and check valid files for changes.

6.1 /tmp/

Since the /tmp/ folder is utilized primiarly to store temporary data, malware or other malicious programs can mount sockets or hide other files in the /tmp/ folder. Use the following command to check for these files.

```
#!/bin/bash
ls -al /tmp/
```

If anything in this folder looks suspicious (or you just want to be safe), create an incident report about the file and run the following command.

```
#!/bin/bash
rm -rf /tmp/<file> # rm -rf /tmp/* to delete
    everything
```

6.2 Root Kit Hunter

rkhunter is a tool used to find root kits on a machine.

```
#!/bin/bash
sudo apt-get install rkhunter
sudo rkhunter --version
```

Use this or the variant for your OS. The second line will make sure it is up to date. The current latest version is 1.4.0.

```
#!/bin/bash
sudo rkhunter --update
```

This line will update the check files for **rkhunter**.

6.3 Installing Anti-Virus

Installing an Anti-Virus on your box will help immensely. They also typically end up as an inject, so installing and running an anti-virus will be helpful no matter what. The one installed will depend on the OS.

6.3.1 Linux

clamav will be used to find infected files on the system.

```
#!/bin/bash
sudo apt-get install clamav
sudo freshclam
```

The pair of commands will install the latest version of **clamav** as well as update all virus definitions.

```
#!/bin/bash
clamscan -r --move=/somewhere / &
```

This command will scan the entire machine, moving any malicious files to a folder called **/somewhere**. The **&** is there to run the command in the background, but this can be accomplished with **tmux** or any other known way.

6.3.2 Windows

Sophos

7 Check cron jobs

Cron jobs are scheduled "jobs" or commands fo rthe server to run automatically at a specified time and date. Malware or the redteam may attempt to use these for persistence mechanisms so clearing them is very important.

To check the cron jobs of a specific user, use:

```
#!/bin/bash
crontab -l <user>
```

To clear any suspicious cron jobs, use:

```
#!/bin/bash
crontab -r <user>
```

8 Checking for Suspicious Programs

Some of the boxes may already be infected and have malicious processes running. To view a list of processes use:

```
#!/bin/bash
ps -eo pid,tty,user,args | less # List all process
    with the following format
```

As a rule of thumb, programs should only be running in **/bin**, **/opt**, **/sbin**, **/usr**.

9 Setup Splunk

10 Setup NTP

NTP stands for Network Time Protocol and runs on port 123. It is used to synchronize computers on a network to UTC time within a few miliseconds. This should not be necessary during CCDC unless there is an inject requiring it, or there is extra time. Keeping similar times on each machine will help with logging and is good practice to have done.

10.1 Creating NTP Server

Choose one of the Linux machines to operate as the NTP server. This machine will be the one acting as the lowest stratum to the rest of the computers. Run the following commands.

```
#!/bin/bash
sudo apt-get install ntp
```

Use the package manager that is on the machine. Next edit **/etc/ntp.conf**. Make sure the following lines are present. They restrict access to clients. Replace the addresses in with the actual subnet of the network given to us. Make sure to delete the brackets.

```
#!/bin/bash
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict {OUR.NET.WOR.K} mask {255.255.255.0} nomodify
    notrap
```

The next lines will use the systems clock in case Internet access is lost.

```
#!/bin/bash
server  127.127.1.0 # local clock
fudge   127.127.1.0 stratum 10
```

Start the service. The NTP server is ready for clients to be configured.

```
#!/bin/bash
sudo service ntp restart
```

10.2 Configuring Clients

The rest of the computers must be configured to use the correct NTP server.

10.2.1 Windows

10.2.2 Linux

All other machines will act as NTP clients. Use the correct package manager for your system.

```
#!/bin/bash
sudo apt-get install ntp
```

Edit the **/etc/ntp.conf** file to add the NTP server to the machine. This line will be added near the top of the file above where the other servers are declared.

```
# Only add the line directly below me
server NTP.SER.VER.IP prefer
server 0.debian.whatever iburst # this is already
   there
```

The next two commands will restart the NTP service, and then list all NTP servers the client sees.

```
#!/bin/bash
sudo service ntp restart
ntpq -p
```

11 Looking at Logs

Look at em

12 Different Attack Vectors

12.1 Bad Binaries

There is always the chance that a binary on your machine can be compromised. At the 2019 CANSEC, our team went up against a network that had tons of bad commands. One machine had the ls binary replaced with the sl binary. This was found through trying to use ls. A different less conspicuous change was passwd, which would change the password, but also open a shell. The only way to check the validity of these commands is to use a tool like rkhunter, which will check the hash of the binary against known good binaries. Typically this should not be seen often, but if something is acting fishy be sure to check.

13 Using Mitnik

Mitnik is the Discord bot that helps out during the competition. He can be used to generate passwords and assist in generating Incident reports. Use **?help** to access his help menu.

13.1 ?genpass

This command will return a new password consisting of a symbol, three words, followed by a number between 00 and 99.

13.2 ?incident

This is the command to use to create, edit and list different incidents.

13.2.1 Create

Create an incident from scratch.

```
?incident -n
```

This will begin an interface with the bot to create a new incident. Follow the prompts on screen while being as descriptive as possible. Everything typed goes straight into the official report, so make it detailed enough to make sense to someone somewhat familiar with the network.

13.2.2 List

List all or a single incident.

```
?incident -l {NUM}
```

Leaving out a specific incident number will list all incidents and their included data. This should be used before editing incidents so the incident number can be found. When run with a number, the command will return only the specified incident.

13.2.3 Edit

Edit an already created incident.

```
?incident -e {NUM}
```

Will edit the specified incident. To find an incidents number, use the list command. Follow the prompts from Mitnik to edit attributes of the incident.s

14 Sources

1. Initial: `http://www.cs.mercer.edu/courses/David%20Cozart/IST%20301/Cyber%20Defense%20Spring%202017/Hardening%20Directives/LinuxGeneralDocumentation-Adams.pdf`
2. NTP: `https://www.thegeekstuff.com/2014/06/linux-ntp-server-client/`