Homework: Unit 6 Advanced Bash: Owning the System

Congratulations! You've made it to the end of the Linux module.

Over these past few weeks, you've played the acted in the role of a systems administrator responsible for diagnosing, securing, and automating the hardening of a compromised Linux host. In doing so, you've explored all of the following, and more:

- The structure of the Linux file system
- What processes are and how to inspect them
- Creating users and groups and editing their permissions
- Scheduling regular jobs with `cron`
- Logging, monitoring, and log analysis
- Automating common tasks with bash scripts, compound commands, and other advanced features of the shell

Getting this far is no small feat. This is truly a wealth of information, all of which is leveraged by professional systems administrators on a near-daily basis.

In this week's homework, we will switch gears and you will play the role of a hacker. You will remotely access a victim's target machine, maintain access via a backdoor, and crack sensitive passwords in the `/etc` directory.

Please fill out the [Submission File](Submission.md) as you complete your homework. This will be your homework deliverable for the week.

You will be learning a lot of new concepts in this homework, and you may need to do a little bit of research. This homework should be a fun, engaging hands-on introduction to maintaining access to a compromised system. You will learn about this in depth during the pentesting units. For now, read the below on Privilege Escalation to better understand the set-up and goal of this assignment.

Privilege Escalation

When an attacker gains access to a machine, their first objective is to always escalate privileges to `root` (which you accomplished during your scavenger hunt activity). When they achieve root privileges, they are able to do anything they want to the system. In cybersecurity parlance, gaining access to a host and escalating to `root` privileges is called **owning the system**.

While owning a system is a crucial piece of the process, it is the first item on an experienced attacker's agenda. Two goals remain on the checklist: **maintaining access** and **exfiltrating data**.

After exploiting a machine, attackers must ensure that they can reconnect at a later date, with the same escalated privileges they attained during the initial assault. This is typically achieved by installing a so-called _backdoor_. A backdoor is any mechanism that allows an attacker to secretly reconnect to a machine they've exploited.

Virtual Machine Set-up

In this homework, you will play the role of a hacker, using the `Attacker Machine` to carry out your activities on the `Target Machine`. If you are using the Vagrant local machine, you will follow the below steps which will simulate a remote machine (the attacker) on the internet that an attacker would use to hack into a organization's servers (the target).

Complete the following steps:

- Ensure that you have `VirtualBox` and `Vagrant` installed on your local machine.

- If your computer has limited resources, make sure you shut down other virtual machines, such as the `Linux` VM and `linux-scavenger` VM as you'll be launching two new ones soon.

- Move the [Vagrantfile](./Vagrantfile) located in this homework directory to your local machine. You can save this file locally to any directory that is **NOT** one of the following as they already have a `Vagrantfile`:

  - `$HOME/Documents/Cybersecurity-Bootcamp/Linux-Module` as this contains your ongoing Linux Ubuntu virtual machine you'll be using again in two weeks.
  - `$HOME/Documents/LabEnvironments/linux-scavenger` as this contains the last activity's virtual machine from your scavenger hunt.

- After saving the `Vagrantfile`, open a terminal window (`Git Bash` for Windows users) and navigate to the directory where you saved this `Vagrantfile`.

- Launch the lab by running `vagrant up`. Leave this `vagrant` terminal window opened.

  - Note that after the machines are set up, you can shut them both down by running the command `vagrant halt`.
  - If you run into any issues at this or any installation step, please reach out to your instructor or TA. This is most likely due to a `root` ownership error.

- Depending on your internet connection and your local machine, it may take a few minutes for `vagrant` and `VirtualBox` to set up your machines, so feel free to grab a cup of coffee while you wait.

- _What's happening_ during this process is that `vagrant` is setting up two `VirtualBox` virtual machines and setting them up with static IP addresses for you to use during this homework.

- After `vagrant` is done setting up the machines, you should now have a `Target Machine` and `Attacker Machine` in your VirtualBox Manager window and both should now be launched.

  ![Attacker and Target Machines in VirtualBox](./Target_Attacker_Machines.png)

Access set-up

To get started by logging into the target machine as `root` do the following:

- Load up your attacker machine and log in with the following credentials:

  - Username: `sysadmin`

  - Password: `cybersecurity`

Begin an `SSH` session into the target machine by doing the following:

- Open a terminal on the attacker machine and run: `ssh sysadmin@192.168.6.105 -p 22`.

This command will attempt to initiate an `SSH` session on your target machine.

- Enter the password `passw0rd` when prompted.

After you've successfully logged into the `sysadmin` account on the target machine, you'll notice your prompt changed to `sysadmin:~\ $ `.

- Swap to the `root` user by entering `sudo -s` and re-entering the password `passw0rd`.

You should now have the `root` prompt `root:~\ $ ` that you acquired during your scavenger hunt activity.

Instructions

Your goal is to *maintain* access to the target machine, by installing a backdoor. You will then use the backdoor to crack sensitive passwords.

To complete this assignment, you must complete a series of steps. Again, some of these steps will require you to research new tools and concepts. Any and all information you might need can be found between the `man` pages and Google searches. Remember: Learning new tools on the job is a key skill for IT and security roles.

Shadow People

In this step, you'll create a "secret" user named `sysd`. Anyone examining `/etc/passwd` will assume this to be a service account, but in fact, you'll be using it to reconnect to the target machine for further exploitation. (Remember that you have alre)

Make sure to give your `sysd` user:

- A password (make sure you remember this)

- A System UID (i.e., any `UID` < 1000 will suffice)

- A GID equal to this UID

- Full, password-less `sudo` access

In addition, minimize exposure by ensuring that your secret user does _not_ have a home folder.

Test that your `sysd` user can execute commands with `sudo` access without a password before moving on.

- Try running `sudo -l` to test. If the terminal does not prompt you for a password, it was a success. Attempt any other commands that require elevated privileges and mark them in your submission file.

Note: that if a hacker can rapidly execute commands on a machine with elevated privileges, then they can more quickly get to exfiltrating important data from the `Target Machine`.

Smooth Sailing

In this step, you'll allow SSH access via port 2222. SSH usually runs on port 22, but opening port 2222 will allow you to log in as your secret `sysd` user without connecting to the standard (and well-guarded) port 22.

To do this you will need to use `nano` to make the appropriate updates to the `/etc/ssh/sshd_config` configuration file that will allow SSH access vis port 2222. When you open the configuration file, add secondary SSH port line _under_ `Port 22`.

This will require some research. Start by examining `/etc/ssh/sshd_config` and using Google or the `man` pages to learn more about the available configuration options.

Testing Your Configuration Update

When you think you've configured things properly, test your solution by testing the new backdoor SSH port. Do the following steps on the target machine:

- First, note that the IP address of the target machine is `192.168.6.105`. You'll need this for when you attempt to log back into the target machine.

- Make sure to restart the SSH service.

- Exit the `root` account, and log off of the target machine (you'll know you're back in your attacker machine when the prompt turns green again).

- Next, you will need to use your attacking machine to test the new backdoor SSH port:

  - SSH back into target machine as your `sysd` user, but this time change the port from 22 to 2222 via: `ssh sysd@192.168.6.105 -p 2222`.

- Once you are connected to the target machine over SSH, use `sudo su` to switch back to the root user.

Note: that this was an important step. You were able to log out of your `root` account, and then _re-establish_ a remote session with escalated privileges through a different, un-guarded port.

Company servers that house sensitive information will often use monitoring and hardening tools to closely watch key ports, such as `22` for `SSH`.

It is also quite difficult for hackers to, on their first breached connection, know where all the most sensitive files exist within a system.

For this reason, hackers need to not only attempt to mask their trails (your `sysd` user), but also ensure they have discreet ways to revisit a system, so that they can maximize the amount of plunder they take from the target machine.

Crack _all_ the things

Next, to strengthen our foothold on this system, we will attempt to crack as many passwords as we can.

Having access to all the accounts will also allow us to access the system if our other backdoors are closed.

- Make sure that you have SSH-ed into the target machine using your `sysd` account.

- Escalate your privileges to the root user.

- Use `John` to crack the entire `/etc/shadow` file.

  - You will not need to transfer the file as `John` is already installed on the scavenger hunt VM.

Note that the reality of cracking passwords is that the process just takes time. Now might be a good opportunity to grab some coffee or take a break and let the computer do the work for you.

Submission

Please finish filling out the Submission.md and submit it for homework upon completion.

Lab clean up

WARNING: ONLY DO THE FOLLOWING ONCE YOU HAVE SUBMITTED YOUR HOMEWORK AND HAVE NO MORE CHANGES TO MAKE TO THIS ASSIGNMENT

These steps are optional if you want to remove the homework-specific `vagrant` lab virtual machines to free up space on your personal computer.

- Within the terminal window that you ran `vagrant up` on (or re-open a terminal window at the directory you saved your `Vagrantfile`):

  - Run `vagrant halt` to shutdown the `Target Machine` and `Attacker Machine` virtual machines.

    - `vagrant` will attempt to gracefully shut down the machines.

  - After that has completed, run the command `vagrant destroy` and confirm removal of both virtual machines by typing `y`/`yes` and hitting enter.