ENPM685 Homework #3 – Penetration Testing

Version 4.0 – February 18th 2022

Estimated time to complete this assignment: 1 hour.

From an unprivileged level of access find a way to elevate your privileges on the Ubuntu host to so you can run commands as root (id 0). There are multiple ways to do this, we discussed a few privilege escalation methods and specific exploits class and in exercises. Do some recon and exploration of the system.

Once you have elevated to root privileges run the **`id`** command to show that you are running as root and then take a screenshot of the output of that command. It should show the following:

```
root@enpm685:/home/admin# id
uid=0(root) gid=0(root) groups=0(root)
root@enpm685:/home/admin#
```

Rules of engagement:

1. You may **NOT** use the account you used to build your VM for this assignment
2. You may **NOT** use the Salt Stack API exploit that we used in class (saltstack_salt_api_cmd_exec)
3. You may **NOT** boot the VM into single user mode
4. You may **NOT** just directly SSH into the system as the **admin** user and sudo to root. You can SSH in as an unprivileged user like **brute** and pivot to the **admin** user (but that's a little boring, see how else you can get to root!
5. Have fun with this assignment!

Deliverables:

1. Your screenshot of the **`id`** command output showing that you are running commands as root.
2. A write up (with supporting screenshots as needed) of how you managed to take your initial access and elevate privileges to run commands as root.