Assignment 4 - Fixing Linux Misconfigurations

For assignment 4, you will be fixing the Linux misconfigurations we set up during class. You must first show me the exploit from class works and you are able to gain root privileges by exploiting them. All fixes should be done on your Ubuntu machine as your Ubuntu administrator account. Then, attempt to exploit using your unprivileged user via SSH or a reverse shell on your Kali machine.

Each section should include a detailed walkthrough with screenshots and short descriptions of your original privilege escalation exploit, all fixes you have made, and evidence that the exploit is fixed - essentially evidence for before, during and after. Please be sure to submit a PDF.

Each section will be scored out of 10 marks:

- Showing the original privilege escalation exploit (2 marks)
- Fixing and showing each step for the privilege escalation vulnerability (5 marks)
- Showing the exploit does not work after fixes (1 mark)
- Report quality (2 marks)

Part 1 - /etc/passwd File with Awful Permissions

You will first show me how your root2 user can ssh into your Ubuntu machine, and their id (using the id command). Then you will remove them from the /etc/passwd file, and change the permissions on the file to the default permissions using chmod. You will then modify your ssh configuration to remove the ability for root users to login, and restart your ssh service. Keep the password authentication for your SSH configuration so that you can complete the following parts.

Part 2 - Cron Jobs with Awful Permissions

You will show me how one of your scripts (bash script or python script) can lead to privilege escalation. Then you will remove any reverse shells from both scripts. You will then modify the permissions with chown and chmod so that root owns both scripts. The permissions should be that root can read, write and execute, the group (root) can only read, and everyone else on the system cannot read write or execute.

Part 3 - Binary without Full Paths

First show me that your binary leads from Module 4 part 2 leads to privilege escalation from your unprivileged user with a malicious nmap binary, and show me your unprivileged user's PATH. Then, remove /var/scripts (or whatever path you had placed your malicious nmap binary in) from your unprivileged user's PATH keeping the default path.Then modify the C code to include nmap and whoami's full path and recompile the binary using gcc. Set the permissions of the binary to be owned by your Ubuntu administrator (the account that can run sudo). It should also have permissions for your administrator to read,write and execute, their group to only read and write, and everyone else on the system to just read and execute. The SUID bit should not be set.

Part 4 - GTFO Bins

Show me how your find and nmap binary can lead to privilege escalation from the perspective of your unprivileged user. Then, remove the SUID bit from find and use visudo to remove the user's ability to run nmap as root without a password. Attempt to run the SUID commands for find, and the SUDO commands for nmap from GTFO bins and show me that you cannot get privilege escalation anymore.