NSS Assignment - 1

Report by Kaustav Vats (2016048)

Part 1
ACL and setuid

In this assignment we were asked to implement ACL which overrides DAC. This assignment was performed on Ubuntu with real user and one Fakeroot. Some of the commands that were implemented in the assignment- Ls, fput, fget, create_dir, do_exec, setacl and getacl.
Each user has home directory inside **fakeslash/fakehome/userDir** with owner as root of directory **fakeslash** and **fakehome.** All binaries has setuid bit enabled and they are owned by fakeroot, which is a root. So whenever a non root user run these binaries then they will run with permission of owner.
Commands:-

- Ls:- List file attributes, ownership, permissions, sizes etc.
- fput/fget:- used to read file or get data from file. (retrieve data based on permissions present in ACL and DAC)
- Create_dir:- used to create a directory
- Do_exec:- used to run binary with that owner permissions.

Acl's are stored using setxattr and getxattr family.

Assumptions-

- No Default permission net be taken from the root directory (Not specified in the Assignment and also confirmed with the professor)
- Can only create one new directory with
- Execute permission should be present for all files. (only read and write need to be changed)

Attacks protection

- Buffer overflow attack
- Do_exec whitelisting
- Handling cases regarding absolute path
- Input filtering

Commands
Directory structure-
Thor (t_file.txt, t_folder)
Batman(b_file.txt, b_folder)
Flash (f_file.txt, f_folder)

- ls <filename>

- ls
- Create_dir absolute path
- Fget <filename>
- Fput <filename> <space spearated string>
- Do_exec <binary> <arguments>
- Getacl <filename>
- Setacl <key> <value> <filename>

Part 2

Written a Linux kernel module that would involve using the netfilter framework. Using `nmap' you we run various kinds of network reconnaissance exercises on the virtual machine.
My module detect

- FYN scan (Only fyn bit enabled)
- SYN scan (only syn bit enabled)
- XMAS scan (FIN, PSH AND URG FLAG SET)
- NULL scan (All bit are disabled)