Introduction to Kali Linux and Vulnerability Assessment Tools

MODULE TOPICS

- Introduction to Kali Linux
- Linux Crash Course

WHAT IS KALI LINUX?

- It is a Debian-derived Linux distribution focusing on
  - Digital forensics
  - Penetration Testing
- A rewrite of BackTrack Linux, a popular penetration testing Linux distro
  - Mati Aharoni
  - Devon Kearns
- Preinstalled with a wide collection of pen testing tools
- Has support for ARM-based hardware platforms
  - Raspberry Pi
  - Chromebook

KALI TOOLS CATEGORY

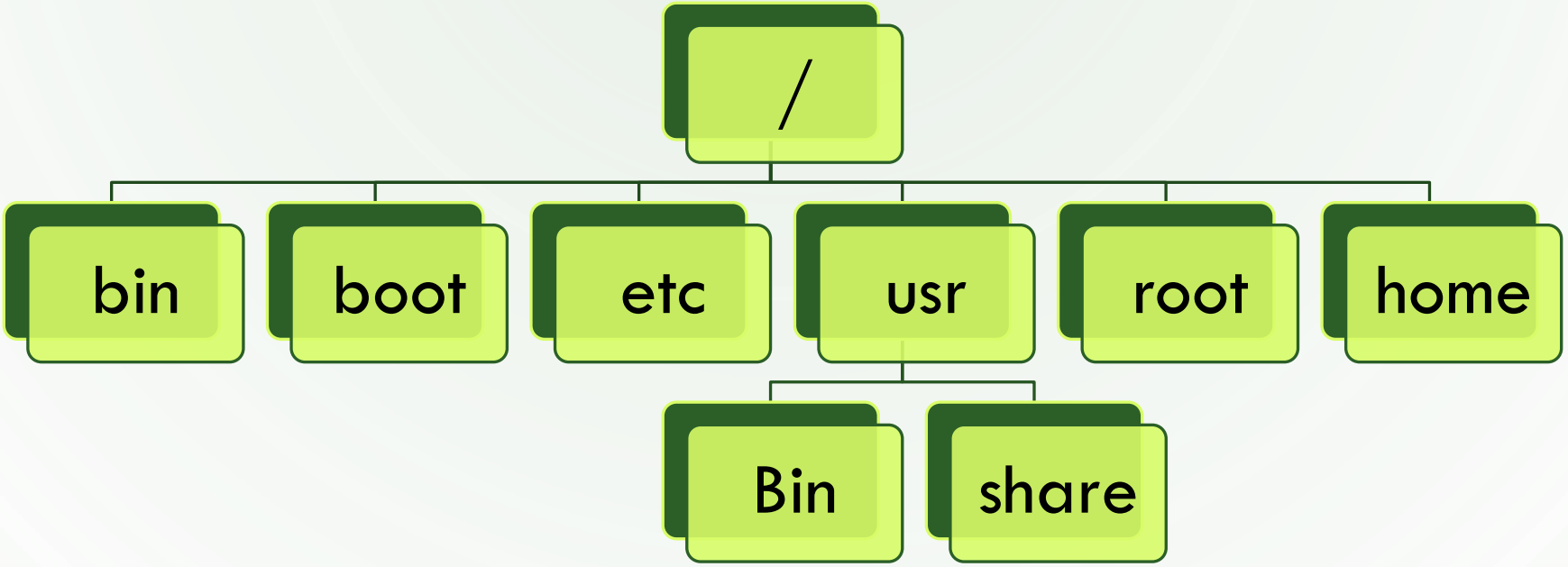
- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress Testing
- Forensics
- Reporting Tools
- Services
- Miscellaneous

NOTE IN USING KALI LINUX

Misuse of security tools within your network, particularly without permission, may cause irreparable damage and result in significant consequences

http://docs.kali.org/introduction/should-i-use-kali-linux

LINUX DIRECTORY STRUCTURE



SOME IMPORTANT DIRECTORIES

- / - root directory
- /bin - binaries/programs that are available to all users
- /etc - system-wide configuration files
- /root - root user home directory
- /home - contains the home folders of all non-root users
- /home/<user> - a user home directory

LINUX SHELL COMMANDS

- **pwd** – print current directory
- **ls** – lists files and folders in a directory
  - **-l** : long listing (detailed)
  - **-a** : shows hidden files
- **Echo <string>** - prints out the specified string
- **cat <filename>** - display contents of file on the screen
- **grep** – does a string search on text output

LINUX SHELL COMMANDS

- **mkdir <name>** - creates a new folder in the current directory
- **cp *or* mv <source> <dest>** - copy or move from source file to destination folder file
- **cd <name>** - moves to another directory
  - **cd ..** – move to parent directory
  - **cd ~** – move to home directory
- **rm *or* rmdir <name>** - remove file/folder
- **man <command>** - bring up the manual page for a command

LINUX SHELL COMMAND OUTPUT REDIRECTION

- >
  - Used to write command output to a file
  - Overwrites the file if it is existing
- >>
  - Used to append command output to a file
- |
  - Pipe character
  - Used to chain the output of a command as the input of the next command

LINUX SHELL COMMANDS FOR NETWORKING

- **ifconfig** –shows the IP address configuration of the host
  - ifconfig <interface> <address> netmask <mask> sets the IP address until next reboot
- **route** – shows the host routing table
  - route add default gw <address> sets the default gateway until next reboot

→ Note: For configs that persist even when rebooted, you must edit the /etc/network/interfaces file

LINUX USEFUL COMMANDS

- **locate/which/find** – used for searching files
- **whoami** – displays the username of the current user
- **hostname** – displays the hostname of the system
- **id** - used to find out user and group names and numeric ID's (UID or group ID) of the current user or any other user in the server
- **last** - displays information about the last logged-in users

LINUX USEFUL COMMANDS

- **ps -** used to list the currently running processes and their PIDs
- **cat /etc/os-release | lsb_release –a | hostnamectl -** find os name and version in Linux:
- **cat /etc/group –** list of groups to which users belong under Linux and UNIX operating system.
- **cat /etc/passwd -** list users on Linux

LINUX USEFUL COMMANDS

- **cat /etc/shadow -** (must be root) list the shadow file which stores the hashed passphrase (or “hash”) format for Linux user account with additional properties related to the user password
- **apt-get –** command used to install / update / remove software packages (needs root privilege)
- **apt-search –** command used to look for available packages

LINUX USEFUL COMMANDS

- **adduser "dlsu-user" –** add user name dlsu-user
- **usermod –aG sudo "dlsu-user" –** add dlsu-user to sudo group
- **sudo –l** or **cat /etc/sudoers –** check the sudoers file

users hosts=(user:group) commands