**PCC: Computer Systems Security**

**Assignment No 1**

**Installation of Virtual Machine with Kali Operating system and study of basic Linux command:**

Because this is largely a hands-on course, it is essential that you learn many of the fundamental Linux commands, an important skill for any good security practitioner. You are strongly encouraged to use the Kali Linux virtual machine for this lab.

Commands: ls, rm, mkdir, rmdir, cd, pwd, ln, chmod, umask, ping, cut, sort, which, grep, whereis, finger, w, who, whoami, last, file, strings, top, ps,nice, nohup, kill, signal, more, less, ifconfig, arp, nslookup, cat, uname, history, netstat, ifconfig, traceroute, dig, man, lsof, whois, crontab, nc, uniq, id, groups, df, du, touch.

In addition, please read "The command-line, for cybersec" by Rob Graham:

http://blog.erratasec.com/2017/01/the-command-line-for-cybersec.html.

Answer the questions below.

1. [Why Does Kali Linux Only Install as root ?](https://docs.kali.org/faq" \l "faq-2307)

Most of the tools require superuser permissions. Hence, the default user is root

1. Which organizations maintains and funds Kali Linux?

Offensive Security

1. **Which is a centralized configuration management service that works with Kali?**

**Advanced Package Management is used in most Debian-based systems.Programs, Libraries and even the kernel itself is managed using APT.**

1. What command can you use to find out your IP address and MAC address?

ifconfig

1. What command can you use to show all the processes that are running on the

system?

ps aux

1. What command can you use to get more details about running processes

listening on ports?

netstat

1. What command with flag could you use to list every file, including hidden files,

on the entire system, showing their owner, location, and access time? Please

also note the flags that you used with command.

ls -la

-l Gives the long description of all files and directories

-a Includes hidden files and directories

1. Assume you found a file named warrent.pdf . What command could you use

to find out what type of file this was?

file warrent.pdf

1. So you discovered that warrent.pdf is a binary executable. What command could you use to extract any readable information from the file without running it? Also, try this on a compressed file such a ZIP or JAR

strings warrent.pdf

1. What command can you use to find the IP address-to-MAC address mappings for systems on the local network?

arp

1. Consider the following IP address: 121[dot]72[dot]232[dot]16. Where is the computer with that IP address located --in what country?

nslookup 121.72.232.16

1. For the previous question, what command did you use to determine the location of the computer?

whois 121.72.232.16 | grep country

geoiplookup 121.72.232.16