# Lab 1 - Host Security and Installation

## Part I

Objective: To Study the concepts of host security by applying some of the industry recommendations for securing a Linux host

1. Set the BIOS password and boot sequence: **Explain why it is necessary to set a BIOS password**
2. Set root password length and expiration time
3. Set login time out for root account
   (How secure a host might be after making all previous recommendations?)

4. Check and disable unnecessary services using inetd
5. make inetd.conf immutable
6. Make /etc/services immutable
   (explain the benefits of making files immutable)

7. Allow root on tty1 only. edit /etc/securetty
8. Disable news, games vendor specific accounts
9. Block su to root for all but members of the wheel group.
10. Put limits on resources. /etc/security/limits.conf
    (Explain why resources need to be limited, what could be the outcome of not having any limits set)

11. Reduce size of the shell history file.
12. Disable Ctl-Alt-Delete
13. Secure scripts under /etc/rc.d
14. Find all SUID GUID programs and files then remove the SUID/GUID bits.
    (Explain the danger of having SUID/GUID files)

15. Briefly explain what a kernel is and major responsibilities
16. Set kernel tunable parameters to adhere to the following restrictions:
    1. Set the kernel parameter to forward Ipv4 packets from one interface to another

2. Set kernel parameter to drop all Ipv4 ICMP echo traffic
3. Set kernel parameter to protect against TCP half open connection attacks.
   (Briefly explain the benefits of previous steps and show how those changes can be made permanent.

## Part II
## Objective: To study the concepts of partitions and filesystem

Setup: CN8822 Virtual machine already has an extra hard disk allocated with 2GB. The virtual SCSI drive is un-partitioned with no filesystem.

1. Find out the device name assigned to this virtual Hard Disk from within the OS
2. Create a new 1G partition
3. Set the partition type to be of SWAP partition
4. Create a swap filesystem on this new partition
5. Attach the new swap partition to the running kernel
   (Explain the benefits of having swap filesystem and show the size of swap used by kernel before and after)
6. Repeat previous steps by creating another 1G partition
7. Set partition type to be a Linux type
8. Create an EXT4 filesystem on new partition
9. Mount new partition as backup with following mount options
   1. No SUID
   2. No Devices
   3. No Execution
   (Explain what each mount option does and recommend other option for this backup partition )