## *Suggested Teaching Guideline for*
## *Network Defense & Countermeasures PG-DITISS September 2022*

**Duration:** 30 class room hrs + 40 lab hrs (Total: 70 Hrs)

**Objective:** To introduce the students to Network Defense and Countermeasures. This includes the following:

- Network Security Concepts,
- Firewalls,
- IDS & IPS, and
- VPN

**Prerequisites:** OS and Network Concepts

**Evaluation method:** Theory Exam: 40% weightage.
Lab Exam: 40% weightage.
Internal Assessment: 20% weightage.

**List of books / Other training Material:**

**Courseware:** Cryptography & Network Security: Principles and Practices by William Stalings.

**Reference:**

- Fundamentals of network and Security: Eric Maiwald/TMH

**Session 1:**

- Introduction to Information Security
- Why Information Security?
- Security: The money factor involved
- Internet Statistics - Study from a security perspective
- Vulnerability, Threat and Risk
- Qos

**Session 2:**

- Risk Management, Exposure and Countermeasure
- Firewall
- De-militarized Zone
- Two methods of implementing firewall

**Session 3:**

- Packet Filtering
- Screened Host Firewall
- Stateful Inspection Firewall
- NextGen Firewall app controls
- iptables - Linux Firewall

**Lab 1:**

- iptables - Rule Processing
- Default Policy
- iptables - Predefined tables
- INPUT
- OUTPUT
- FORWARD

**Lab 2:**

- Iptables / netfilter/ Xtables-Addons
- verifying iptables / netfilter
- internal working
- iptables / netfilter - concept of targets
- DROP
- ACCEPT
- iptables - SPI Firewall
- Setting up a SPI Firewall - Standard installation
- Iptables IPv6 Rule Management

**Lab 3:**

- Automating iptables and scripting
- Bash Scripting to automate iptables
- Advanced iptables
- Loading of modules
- Geo IP Blocking using Xtables-Addons

**Lab 4:**

- Access control using iptables
- Internet sharing Using Iptables

**Session 4:**

- Wireshark
- Create a filters for data collection and display
- Examine real-world packet captures

**Lab 5:**

- Wireshark
- Examine real-world packet captures
- Iptables Port Forwarding
- Iptables use case: Fail2ban

**Session 5:**

- Linux Software Firewall(ClearOS Pfsense)
- Nginx & Squid Reverse Proxy
- UTM
- Server Load Balancing

**Lab 6 & 7:**

- Nginx & Squid Reverse Proxy
- Configure reverse proxy URL using regex
- Server Farming

**Session 6 & 7:**

- VPN – Introduction
- VPN protocols/characteristics
- VPN Functions
- Types of VPN
- SecureVPN
- Trusted VPN

**Lab 8 & 9:**

- OpenVPN configuration in both Linux & Windows
- Site to Site Connectivity
- Certificate & Password dependent authentication
- VPN configuration for Mobile Device

**Lab 10:**

- Pfsense OS - Installation and Configuration
- Installation of Pfsense OS and Basic
- Configuration

**Lab 11:**

- UTM Configuration
- Basic Setup of UTM

**Lab 12:**

- Configuration for access control and Firewall features (UTM)
- UTM VPN Configuration

**Session 8:**

- Hybrid VPN
- IPsec
- Tunnel mode/transport mode
- Ipv6 VPN
- Split Tunnel full tunnel VPN

**Lab 13 & 14:**

- VPN Configuration under Windows 2016 using RRAS
- L2TP/PPTP VPN Setup

**Session 9:**

- Introduction to IDS and IPS
- IDS / IPS
- Types of Attacks
- IDS
- Security Events
- Vulnerability/design/implementation

**Lab 15 & 16:**

- Distributed Honeynet System (Developed by C-DAC)
- Dynamically configure Honeypot
- UAC (URL Analyzer and Classifier)
- Tcpdump installation, verification and basic usage of tcpdump

**Session 10:**

- Attacks-traditional/distributed
- Intruder types

**Session 11:**

- Types of IDS
- IPS categories
- Defence in depth
- IDS and IPS analysis scheme
- Detection methodologies
- Principles of IDS

**Session 12:**

- Symptoms of attacks
- Tired architecture
- Sensors-network/host based
- Denial of services
- Dos & DDos Mitigation

**Session 13:**

- Sensor Deployment
- Agents
- Functions of IDS agents
- IDS Manager

**Session 14:**

- Introduction of Log Analyser
- Log
- SIEM Log Correlation and event triggering
- Introduction of SIEM
- SIEM Log Forwarding Configuration
- SIEM Log Correlation and event triggering

**Lab 17 & 18:**

- Snort
- Writing Basic Snort Rules
- Syslog Server
- BASE
- Configuration and deployment of SIEM

**Session 15:**

- Testing Snort in both Windows & Linux
- IDS architecture
- Bypassing an IDS

**Lab 19 & 20:**

- Testing of Snort using a simulated attack
- Nagios
- Nagios Sensor Configuration (Windows & Linux)
- Nagios with Email services
- Nagios with up/Down of Ram/Hard Disk