

Suggested Teaching Guidelines for
Security and Traffic Management – PG-DHPCSA August 2019

Duration: 30 class room hrs. + 40 lab 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: CCEE Theory Exam: 40% weightage
Lab Exam (Case Study based): 40% weightage
Assignments: 20% weightage

List of books / Other training Material:

Text book: No specific courseware for modules, faculty may share some course materials.

Reference:

- Network Defense and Countermeasures: Principles and Practices by William (Chuck) Easttom/ Pearson
- Cryptography & network Security: Principles And Practices, 4/e by William Stallings,
- 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
- Firewall type

Session 3:

- Packet Filtering
- Screened Host Firewall
- Bastion host
- Stateful Inspection Firewall
- iptables - Linux Firewall
- TMG Threat Management Gateway

Suggested Teaching Guidelines for

Security and Traffic Management – PG-DHPCSA August 2019

Lab Assignment:

- iptables / netfilter
- verifying iptables / netfilter
- internal working
- iptables / netfilter - concept of targets
- DROP
- ACCEPT
- iptables - Predefined tables
- INPUT
- OUTPUT
- FORWARD
- iptables - Rule Processing
- Default Policy
- Processing Order and common mistakes
- iptables - SPI Firewall
- Setting up a SPI Firewall - Standard installation
- Automating iptables and scripting
- Bash Scripting to automate iptables
- Advanced iptables
- Loading of modules
- State
- Access control using iptables
- Internet sharing Using Iptables
- Threat Management Gateway (TMG) Installation & Configuration
- Installation on Windows 2012 Server
- Client Share Installation

Session 4:

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

Lab Assignment:

- Wireshark
- Examine real-world packet captures

Session 5:

- Linux Software Firewall (ClearOS / Untangle)
- Nginx & Squid Reverse Proxy
- UTM
- VPN – Introduction

Lab Assignment:

- Nginx & Squid Reverse Proxy
- Server Farming

Session 6:

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

Suggested Teaching Guidelines for

Security and Traffic Management – PG-DHPCSA August 2019

Lab Assignments:

- OpenVPN configuration
- Site to Site Connectivity
- Certificate & Password dependent authentication
- VPN configuration for Mobile Device
- Clear OS - Installation and Configuration
- Installation of Clear OS and Basic Configuration
- UTM Configuration
- Basic Setup of UTM
- Configuration for access control and Firewall features (UTM)
- UTM VPN Configuration

Session 7:

- Hybrid VPN
- IPsec
- Tunnel mode/transport mode
- Ipv6 VPN

Session 8:

- HMAC
- Crypto Choices
- VPN Implementation using L2TP/PPTP

Lab Assignment:

- VPN Configuration under Windows 2012 using RRAS
- L2TP/PPTP VPN Setup

Session 9:

- IDS / IPS
- Types of Attacks

Lab Assignment:

- Configuring TMG (Windows) as an IDS

Session 10:

- IDS
- Security Events
- Vulnerability/design/implementation

Lab Assignment:

- Tcpdump
- installation, verification and basic usage of tcpdump

Session 11:

- Attacks-traditional/distributed
- Intruder types
- Introduction to IDS and IPS

Session 12:

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

Suggested Teaching Guidelines for

Security and Traffic Management – PG-DHPCSA August 2019

- Principles of IDS

Session 13:

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

Session 14:

- Sensor Deployment
- Agents
- Functions of IDS agents

Lab Assignment:

- Snort
- Writing Basic Snort Rules
- BASE

Session 15:

- IDS manager
- Nagios
- Testing Snort
- IDS architecture
- Bypassing an IDS

Lab Assignment:

- Testing of Snort using a simulated attack
- Nagios
- Nagios Sensor Configuration (Windows & Linux)