Advance Security System

Objective: Advanced Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Topics to be covered in Workshop

1. Defining Security

2. Layered Security - Application Layer/ Session Layer/ Network Layer/ Host Layer (Physical Layer)

3. Sources of Threat to Network

a. Sources of External Threats

b. Sources of Internal Threats

4. Secure Network Layouts/ Architecture

5. Basics of various devices (Networks + Security) - Routers, Switches, Firewalls, IPS/IDS, UTM

6. Network Security Devices - Firewalls, NIPS/ NIDS, UTM (Unified Threat Model)

7. Network Security

A. Port Scanning - Vulerability Assessment

B. Network Mapping

C. Spoofing

i. TCP Spoofing

ii. DNS Spoofing

iii. IP Spoofing

iv. Web spoofing

D. Hands-On

i. Detecting Spoofed Emails/ Websites

E. DOS Attacks

i. SYN Flood Attacks

ii. SMURF Attacks

iii. UDP Flood Attacks

F. Hands-On

i. Handling a DOS Attack

ii. DoS Defence Strategies

iii. Using System Logs to Detect a DOS Attack

G. Secure Remote Access

i. Introduction

ii. VPN's

H. Remote User Authentication

i. RADIUS

ii. Kerberos

iii. CHAP

8. Wireless Security

A. 802.11 Wirless Standards

B. Wireless Network Vulnerabilities

a. Signal Bleed and Insertion Attacks

b. Signal Bleed and Interception Attacks

c. SSID Vulnerabilities

d. DOS

e. Battery Exhaustation Attacks

C. Wireless Security Provisions

a. 802.11x Security

9. Firewalls

A. Types of Firewalls - Packet Filtering/ Proxy Firewalls/ Application Firewalls

B. Firewall RuleSet (Standard + Customised)

C. Firewall Features

a. Statesful Inspection

b. Deep Packet Inspection

D. Logging in Firewall and Log Analysis of Firewall

E. Firewall Log Reporting Tools

F. Hands-ON of the CheckPoint Firewall Management Console.

10. NIPS - (Network Intrusion Prevention Device)

A. What is IPS Device

B. Depolyment to facilitate Network sEcurity

C. Modes of Operation

D. IPS Signature Tuning

E. IPS Screenshots - Attack Attempts/ Configuration Parameters

11. UTM - (Unified Threat Model)

A. What is UTM

B. Utilities in UTM

C. Features of UTM

D. DLP - Data Leak Prevention

12. VPN - Virual Private Network

A. What is VPN

B. How Security is ensured in VPN

C. Mode of Operation of VPN

13. Hands-on the Tools

A. Tennable Nessus

B. NexPose

14. Malwares

A. Malware Types

B. How AntiVirus Works

C. Gateway Level AntiViruses-UTM Component

15. Encryption

A. Introduction

B. Types-Symmetric Key, Assymetric Key, Hashing

C. Encryption in E-Commerce

D. Difference between HTTP and HTTPS

E. Concept of Digital Certificates - how they ensure Security

F. Hands-On

a. MD5 generator