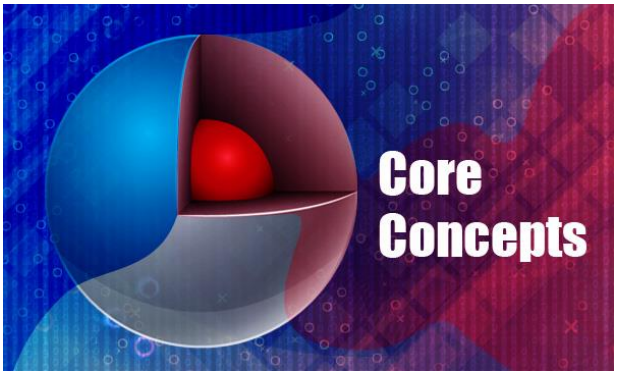
ECC Core Concepts – IT Security



Course Outline:

Module 01: Introduction To Required Skills For Security

- TCP/IP
- Unix/linux
- Introduction to the hacking process
- Virtualization

LAB: Security Skills Introduction

Security Model

- Authentication
- Confidentiality
- Integrity
- Availability
- Authorization

LAB: Security Model

Security Posture

- Promiscuous
- Paranoid
- Permissive
- Prudent

Security policy

- Identifying services and allowing them

Risk Management

- Defining types of risk
- Types of risk

Module 02: TCP/IP 101

Introduction & Overview

- Introducing TCP/IP networks
- What TCP/IP Networks
- What TCP/IP provides: Key application services & multivendor capabilities TCP/IP & the internet
- Internet RFC's & STDs
- TCP/IP Protocol architecture
- Protocol layering concepts
- TCP/IP layering
- Components of TCP/IP networks
- Network protocols (IP, TCP, UDP, ICMP)

LAB: TCP/IP

Transport protocols

- Packet headers

Encapsulation

LAB: The Layers

Analyzing Network Traffic

- Examining the data at the packet level
- Control flags of TCP

Identifying the characteristics of network connections

LAB: Analyzing Packets

Advanced Protocol Analysis

Using Protocol Analyzers

- tcpdump
- dsniff
- Wireshark
- Etherape
- Ettercap

LAB: Protocol Analysis I

Wireshark

- Leveraging the filter capabilities
- Working within the GUI
- Low level analysis
- Following session communication
- Customizing the interface
- Using the statistics features within the tool
- Text-based Wireshark
- Packet decomposition

LAB: Protocol Analysis II

Tcpreplay

- Using traffic replay for training & advanced analysis

Customizing & crafting packets

- Command line tools
- GUI based tools

LAB: Protocol Analysis III

Advanced features of Wireshark

- Filters
- Sessions
- Graphs
- Endpoints
- Statistics
- Custom

LAB: Advanced Wireshark

- Colasoft
- Hping

LAB: Crafting Packets

Module 03: Introducing Linux

- Interacting with UNIX
- Graphical user interfaces
- The Common Desktop Environment (CDE)
- GNOME, Java Desktop System, others
- The command line interface
- Entering commands to the shell
- Browsing online documentation
- Displaying **man** pages
- Managing Files
- Essential file housekeeping tools
- Copying: **cp**
- Renaming: **mv**
- Removing: **rm**
- Linking: **ln**

- Editing: **vi**
- Printing: **lp, lpr**

Root

- Ways to assume root

Lab: UNIX I

Working with the processes & jobs

- ps
- jobs
- kill

Disk Commands

- Mount
- Unmount
- df
- du

Working with files

- gunzip
- zcat
- tar

Searching files & directories

- find
- grep
- strings

Compiling programs

Password storage

Networking

Address resolution

Editors

Lab: UNIX II

Module 04: Introducing Linux

- The UNIX heritage
- Linux inception
- Linux kernel & GNU tools
- Open source licensing
- Distributions
- Accessing the system
- The GNOME desktop
- Customizing panels, launchers & applets
- Examining graphical applications
- Personalizing the terminal window
- Starting at the command line

LAB: Linux

Module 05: Overview of Virtual Machines

- Defining virtual machines (servers & workstations)
- Advantages of deploying VMs
- Creating a Virtual Machine from a System Image or Another Virtual Machine
- Conversion Process for Importing from Other Formats
- VMware Converter Compared to the Conversion Wizard
- Supported Source machines
- Operating System Compatibility
- Importing from Various Sources

Transferring Files & Text Between the Host & Guest

- Using drag-and-drop
- Enable or disable drag-and-drop
- Using copy & paste

- Enable or disable copy & paste
- Using shared folders
- Set up shared folders
- Enabling and disabling shared folders
- Viewing a shared folder

Preserving the State of a Virtual Machine

- Using the suspend & resume features
- Use hard suspend or soft suspend
- Suspend or resume a virtual machine
- Using snapshots
- Scenarios for using multiple snapshots
- Information captured by snapshots
- Snapshot conflicts
- Enable or disable background snapshots exclude a virtual disk from snapshots 193
- Snapshot manager overview
- Take a snapshot
- Rename a snapshot or recording
- Restore an earlier state from a snapshot
- Delete a snapshot or a recording
- Take or revert to a snapshot at power off

Configuring a Virtual Network

- Components of the virtual network
- Virtual switch
- DHCP server
- Netwrok adaptor
- Common networking configurations

Building complex virtual architectures to emulate enterprise architectures

Module 06: Introduction to Vulnerability Assessment

- Defining vulnerability
- Vulnerability scanners
- Challenge of vulnerability assessment
- Penetration testing defined

- Enumeration

Module 07: Introduction to the Hacking Process

Hacking Methodology

- Surveillance
- Foot printing
- Scanning
- Vulnerability assessment
- Exploitation
- Covering tracks
- Evasion

Module 08: Challenges of Staying Current

Refrences

- Books
- Mailing lists
- Videos
- Professional organizations