LINUX Security, Firewalls & Proxies

Introductory Course

Course Title

- Introduction to LINUX Security Models

Objectives

- To understand the concept of system security
- To understand the need for secured systems
- Introduction to Intrusion Detection, Firewalls & Proxies

Introductory Course…

Training Road Map

- Understanding the security triangle – confidentiality, integrity & availability
- Introduction to Linux Security Model
- Traditional Security Architecture
- Authentication & access control mechanisms
- Secure Operating Systems
- Partitioning and File System Security
- Security Updates
- Log Concept
- Services and Protocols
- Secure remote administration

Introductory Course…

Training Road Map…

- Firewall
  - Introduction
  - TCP/IP Recap
  - iptables (Netfilter)
  - Implementation
  - Management
- Proxies
- Simulated Attack

Introductory Course…

- Duration
  - 8 hours (6 hours lecture + 2 hours laboratory)
- Pre-requisites
  - Basic LINUX commands
- Trainer requirement
  - Good understanding of the LINUX System
  - Advanced LINUX commands
  - System Administration
  - Understanding on Networking concepts, IP addresses, subnets, etc
  - Excellent understanding of security models & their implementation

Introductory Course…

- System requirements
  - Hardware
    - Cluster (independent of the main network) with atleast two server nodes
    - Terminal for each participant
  - Software
    - OS
    - Tools for ethical hacking
    - Firewall
    - Proxy
    - IDS / IPS

Introductory Course…

- Course material

Linux security – Intermediate

Course Title

- LINUX Security - Intermediate

Objectives

- To understand the concept of system security
- To understand the need for secured systems
- To be able to implement Intrusion Detection, Firewalls & Proxies

Linux security – Intermediate

Training Road Map

- Understanding the security triangle – confidentiality, integrity & availability
- Introduction to Linux Security Model
- Traditional Security Architecture
- Authentication & access control mechanisms
- Partitioning and File System Security
- Security Updates
- Log Concept
- Services and Protocols
- Secure remote administration

Linux security – Intermediate

Training Road Map…

- Cryptography Basics
- SSL and VPN
- Securing Remote Access into the server
- Securing Apache
- Application-Level Gateway Basics
- IDS and IPS

Linux security – Intermediate

Training Road Map…

- Firewall
  - Introduction
  - Need for firewall
- TCP/IP concept recap
  - TCP/IP model
  - Common protocols - TCP, UDP, IP, ICMP
  - TCP 3 way handshake

Linux security – Intermediate

Training Road Map…

- Firewall…
  - Types of firewalls
  - Working principles (at what level / layer does it do the checking)
  - Software / hardware based firewall
  - Packet filtering
  - iptables basic configurations and usage, chains
  - Practical implementations
  - firewall management (using firewall script / ruleset software)
  - GUI based / web based

Linux security – Intermediate

Training Road Map…

- Firewall…
  - Further reading/discussion
  - Firewall, why is it not enough
  - Other threats that cannot be detected
  - Firewall, as one of the options, not a means to solve security problems
  - sample of combination with firewall usage
  - IDS ? IPS ? what next? Proxies

Linux security – Intermediate

- Proxies
  - Introduction
  - Configuring
- Audit and Log

Linux security – Intermediate

- Duration
  - 24 hours (18 hours lecture + 6 hours laboratory)

- Pre-requisites
  - Basic LINUX commands
- Trainer requirement
  - Good understanding of the LINUX System
  - Advanced LINUX commands
  - System Administration
  - Understanding on Networking concepts, IP addresses, subnets, etc
  - Excellent understanding of security models & their implementation

Linux security – Intermediate

- System requirements
  - Hardware
    - Cluster (independent of the main network) with atleast two server nodes
    - Terminal for each participant
  - Software
    - OS
    - Tools for ethical hacking
    - Firewall
    - Proxy
    - IDS / IPS

Linux security – Intermediate

- Course material

Linux security – Advanced

Course Title

- LINUX Security - Advanced

Objectives

- To understand the concept of system security
- To understand the need for secured systems
- To be able to implement Intrusion Detection, Firewalls & Proxies
- To understand possible vulnerabilities of unstable proxies and solutions

Linux security – Advanced

Training Road Map

- Understanding the security triangle – confidentiality, integrity & availability
- Introduction to Linux Security Model
- Traditional Security Architecture
- Authentication & access control mechanisms
- Secure Operating Systems
- Partitioning and File System Security

Linux security – Advanced

Training Road Map…

- Security Updates
- Log Concept
- Services and Protocols
- Secure remote administration
- Vulnerabilities, threats & exploits

Linux security – Advanced

Training Road Map…

- Cryptography Basics
- SSL and VPN
- Securing Remote Access into the server
- Securing Apache
- Application-Level Gateway Basics
- IDS and IPS
- Security awareness, Security policies, Security implementation & Change Management

Linux security – Advanced

Training Road Map…

- Firewall
    - Introduction
    - Need for a firewall
- TCP/IP concept recap
    - TCP/IP model
    - Common protocols - TCP, UDP, IP, ICMP
    - TCP 3 way handshake

Linux security – Advanced

Training Road Map…

- Firewall…
  - Types of firewalls
  - Working principles (at what level / layer does it do the checking)
  - Software / hardware based firewall
  - Packet filtering
  - iptables basic configurations and usage, chains
  - Practical implementations
  - firewall management (using firewall script / ruleset software)
  - GUI based / web based

Linux security – Advanced

Training Road Map…

- Firewall…
  - Further reading/discussion
  - Firewall, why is it not enough
  - other threats that cannot be detected
  - as one of the options, not a means to solve all security problems
  - sample of combination with firewall usage
  - IDS ? IPS ? what next? Proxies

Linux security – Advanced

- Proxies
  - Intoduction
  - Configuring
  - Vulnerabilities of unstable proxies & solutions
- Audit and Log
- Database level security
- Introduction to Ethical Hacking
- Analysing your server security (e.g.: detecting/preventing Trojans, backdoors, bruteforce attack)
- DDoS attack

Linux security – Advanced

- Duration
  - 10 days (each day with 6 hours lecture + 2 hours laboratory)

- Pre-requisites
  - Basic LINUX commands
- Trainer requirement
  - Good understanding of the LINUX System
  - Advanced LINUX commands
  - System Administration
  - Understanding on Networking concepts, IP addresses, subnets, etc
  - Excellent understanding of security models & their implementation

Linux security – Advanced

- System requirements
  - Hardware
    - Cluster (independent of the main network) with atleast two server nodes
    - Terminal for each participant
  - Software
    - OS
    - Tools for ethical hacking
    - Firewall
    - Proxy
    - IDS / IPS

Linux security – Advanced

- Course material

Thank You