TK012: Linux Security

Duration

5.0 Days

Course Content

1. Security Basics

- 1.1. What is Security?
- 1.2. Assessment
- 1.3. Prevention
- 1.4. Detection
- 1.5. Reaction

2. Threats and Risk Assessment

- 2.1. Classes of Attackers
- 2.2. Types of Attacks
- 2.3. Trade Offs

3. Physical Access

- 3.1. Physical Security
- 3.2. Hardware Security
- 3.3. Understanding the Linux Boot Process

4. Logging

- 4.1. Logging Overview
- 4.2. Syslog Services
- 4.3. The Linux Kernel Audit Daemon

Copyright © TEKonsult 2017

4.4. Linux Firewall Logging

4.5. Log Reports

5. Auditing and Detection

5.1. Auditing Basics

5.2. Understanding an Attack Progression

5.3. Detecting an Attack

5.4. Intrusion Detection Systems

6. Application Security

6.1. Bugs and Tools

6.2. Tracking and Documenting Changes

6.3. Resource Access Control

6.4. Mitigation Techniques

6.5. Policy Based Access Control Frameworks

6.6. Real World Example

7. Kernel Vulnerabilities

7.1. Kernel and User Spaces

7.2. Bugs

7.3. Mitigating Kernel Vulnerabilities

7.4. Vulnerabilities Examples

8. Authentication

8.1. Encryption and Authentication

8.2. Passwords and PAM

8.3. Hardware Tokens

8.4. Biometric Authentication

Copyright © TEKonsult 2017

8.5. Network and Centralized Authentication

9. Local System Security

9.1. Standard UNIX Permissions

9.2. Administrator Account

9.3. Advanced UNIX Permissions

9.4. Filesystem Integrity

9.5. Filesystem Quotas

10. Network Security

10.1. TCP/IP Protocols Review

10.2. Remote Trust Vectors

10.3. Remote Exploits

11. Network Services Security

11.1. Network Tools

11.2. Databases

11.3. Web Server

11.4. File Servers

12. Denial of Service

12.1. Network Basics

12.2. DoS Methods

12.3. Mitigation Techniques

13. Remote Access

13.1. Unencrypted Protocols

13.2. Accessing Windows Systems

13.3. SSH

Copyright © TEKonsult 2017

13.4. IPSEC VPNs

14. Firewalling and Packet Filtering

14.1. Firewalling Basics

14.2. iptables

14.3. Netfilter Implementation

14.4. Netfilter rule management

14.5. Mitigate Brute Force Login Attempts

15. Response and Mitigation

15.1. Preparation

15.2. During an Incident

15.3. Handling Incident Aftermath

Copyright © TEKonsult 2017