ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Linux Security

Course Summary

Description

As Linux (and its derivatives) has proven to be the most deployed Operating System on the planet, it does not come free of risks. Moreover, given its roots as a General Purpose Operating System, some tradeoffs must be made between security and usability. In addition to that, being an ever-evolving Open-Source ecosystem, it's hard to keep track of the latest tools, latest bug fixes, latest bugs introduced, and best practices and configuration options.

In this intensive hands-on course, which is targeted mainly towards System Administrators and Field Support Engineers—you will learn to analyze and mitigate the risks involved with your Linux product.

Objectives

By the end of this course, students will be able to:

- Understand the attack vectors applied on Linux systems
- Understand how to configure your systems for the highest protection levels
- Feel comfortable with kernel parameter configurations via sysfs tools
- Understand how to monitor activities, find irregularities and handle them
- Understand how to protect your user's data
- Analyze threats and risks, suggest mitigation tools and devise policies

Topics

- Introduction to Security
- Linux Startup and monitoring
- Binary level and OS level Security
- Access Control
- Applied Cryptography
- System Level Network Security
- Linux Hardening
- Introduction to Malware Analysis
- Introduction to Android Security

Audience

System Administrators and IT managers as well as Integrators and Field Support/Application Engineers who are interested in understanding and hardening their deployed Linux based products (Servers, IoT end-points)

Prerequisites

To take this course, you must know your way around a modern Linux distribution. You should be able to answer most of the following questions:

- How do you use the following commands: ls, ps, cp, mv, pwd, cat, chmod, chown, mount, etc.
- How to add, remove and modify user accounts
- What is the init process?
- What are users and groups in Linux and how do r/w/x permissions work?

Duration

Five days

ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Linux Security

Course Outline

I. Introduction to Security
- A. Introduction to Security
- B. Legacy and modern threats
- C. Physical and Hardware Security
- D. Cyber Security terminology
- E. Real-time attack map demonstration. Why and who should be worried
- F. Present-time attack vectors
- G. Present-time defense solutions

II. Linux Startup and monitoring
- A. The Linux boot sequence: from power on to login
- B. Linux logging, syslog, kernel audit, system component log reports
- C. Linux networking and monitoring tools
- D. Auditing and detection
- E. Service management and configuration (initd/upstart/systemd)
- F. User management in Linux, the root user and sudo-ers.
- G. Introduction to on host and on network firewalls and Intrusion Detection Systems

III. Binary level and OS level Security
- A. The Gnu Compiler Collection (GCC) framework.
- B. Binary exploitation: Buffer Overflow, Format string errors, integer overflow
- C. Shellcode techniques: Constructions and identification
- D. Heap overflows and heap spraying techniques
- E. Kernel vulnerabilities and bugs, reacting to such
- F. GCC binary code protection techniques and flags
- G. Kernel and userspace process level protection: ASLR, PIE, DEP

IV. Access Control
- A. Discretionary Access Control (DAC)
- B. Permission system, privilege escalation, setuid/setguid exploitation techniques
- C. Linux Capabilities
- D. Mandatory Access Control (MAC), domain specific policy enforcement
- E. Access Control Lists (ACL)
- F. SELinux , Mandatory Access Control (MAC) and domain specific policy enforcement
- G. SELinux MAC alternatives and relaxations: AppArmor, SMACK
- H. Linux resource and user monitoring
- I. Off device access: Forensics tools and anti-forensics techniques

V. Applied Cryptography
- A. Cryptography goals: Authentication, Integrity, Encryption.
- B. Symmetric and Asymmetric cipher suites
- C. Random numbers, Pseudo Random Number Generation
- D. Key generation techniques and trade-offs
- E. Software vs. Hardware based techniques
- F. Cryptography libraries
- G. System wide Trusted Execution Environment/Platform Module integration
- H. File system encryption, trusted boot
- I. The openssl and openssh frameworks
- J. Java* security, keytool, jarsigner and the Java Cryptography Extensions (optional)
- K. Passwords generation and biometric authentication
- L. Network tools

Linux Security

Course Outline (cont'd)

VI. System Level Network Security
- A. Network privacy dangers: Packet sniffers and interceptors. MITM attacks
- B. Certificate Authority (CA) Chain of trust: A solution and the introduced problems
- C. Secure communication with TLS/SSL
- D. Encrypted network privacy dangers: Sniffers and interceptors. MITM attacks
- E. Application network security constraints, and attack scenarios
- F. Application CA management, trusted certificate and pinning techniques
- G. IP layer security, VPN and IPSEC tools.
- H. Network Services security, local and remote servers.
- I. Remote invocation, sniffing and mapping tools
- J. DOS (Denial of Service) attacks, bugs and mitigation techniques

VII. Linux Hardening
- A. The hardening lifecycle: Configuring, auditing, detecting, mitigating, patching
- B. Firewalls and packet filtering: Nftables, netfilter, iptables
- C. Intrusion Detection/Prevention Systems (IDS/IPS): Snort, Suricata, OSSEC
- D. Linux Kernel configuration hardening
- E. Linux service configuration hardening
- F. Package sources and component selection
- G. Advanced Linux configuration tools, procfs, sysfs, debugfs
- H. Linux service selection and hardening
- I. Apache and Nginx web server hardening
- J. Linux user management
- K. Filesystem selection: confidentiality, integrity, and performance considerations.
- L. sysfs access restrictions
- M. MAC policies and strategy
- N. Software patches and update policies. Support channel strategies
- O. Virtualization and light virtualization: Virtual Machines, namespaces, containers.
- P. Honeypot techniques

VIII. Introduction to Malware Analysis
- A. Testing environment considerations, Virtual Machine detection techniques
- B. Malware terminology
- C. Malware mutation, obfuscation, packaging
- D. Malware classification and research strategy: Fingerprint, instrument, reverse
- E. Fingerprinting techniques
- F. Behavioral (Dynamic) analysis techniques, Process and OS instrumentation
- G. Static analysis techniques, reverse engineering
- H. Taking it from here: Going beyond the intro

IX. Introduction to Android Security
- A. The Android init process and comparison to Linux
- B. Android security model and comparison to Linux
- C. SELinux implementation in Android
- D. Chain of trust model and certificate attacks
- E. Binary exploitation attacks
- F. Taking it from here: Going beyond the intro