Linux OS Security Introduction

Table of Contents

Linux Operating System Security ........................................................................................................... 2
Course Objectives -1 .............................................................................................................................. 3
Course Objectives -2 .............................................................................................................................. 5
Course Agenda ..................................................................................................................................... 6
Notices ................................................................................................................................................... 7
001 Jeff Arsenault: All right, good morning. Welcome to Linux Operating System Security. I’m your instructor, Jeff Arsenault.
Course Objectives -1

Understand the Linux security model and its key components like process security, kernel tuning, daemons, and chroot jails

Use and configure users, groups, and file permissions as well as describe best practice recommendations

Identify the common attacks seen in a Linux environment

Understand software repositories and updating installed programs

**004 Course Objectives

So like the name says-- so we're going to understand the Linux security model, its key components; talk about process security, how to tune the kernel for security, keeping security in mind the whole time. Daemons or equivalents like services in Windows.

How to configure user groups and the permissions on them, along with your files.

And we're going to talk about some of the common attacks that we see in the Linux environment. They're a little bit different than what we see in the Windows environment.
And how to manage the infrastructure- how to-- patch management, how to install packages, the repositories.

For this- for this class we're going to focus on Red Hat Enterprise Linux 6. That's going to be what everything is geared towards. And a few of the examples we do gives-- like in the software repository section we talk a bit about how Ubuntu works and Debian. But for most parts everything's going to be assuming Red Hat Enterprise Linux 6.
Course Objectives -2

Describe security functions and features in wired and wireless networking

Demonstrate select security features in Linux such as the iptables firewall, anti-malware, and logging and auditing functions

Understand the available guidance on hardening Linux from a security perspective

Explain the BASH shell and its use in scripting security configuration and review

**005 We’re going to cover the network side of it with the wired and wireless networking; the security of those.

Talk about iptable firewalls, one of the most important parts of security.

Antimalware is limited on the Linux environment but there are still possibilities out there; and there is software that can help mitigate that. All important: logging and auditing for identifying if you had security issues on your systems.

We’re going to talk about some of the available guidance out there for best practices.
And then we're going to cover a little bit of scripting. We're not going to get into actual-- we're not going to get too complicated. But we're going to give some examples of how BASH scripting works and-- to do security monitoring and how to automate functions, common functions.

**Course Agenda**

Welcome and Introductions
Security Model
Users and Groups
Threats and Vulnerabilities
Distributions and Software Updates
Networking and Wireless Security
Security Features
BASH Scripting
Hardening

**006 So all that's going to be covered in this agenda. That's what we just did. This is going to be the Welcome and Introductions. And we'll cover the Security Model and Users and Groups today. And then tomorrow we'll get into Threats and Vulnerabilities, Distribution and
Software Updates and Network and Wireless Security and Security Features. And then the last day we'll continue with Linux security features, scripting and hardening- our BASH scripting and hardening.

So it's a lot of information over the next three days. I've got a lot of slides. But I'm going to try not to linger on the slides.

Notices

© 2013 Carnegie Mellon University

This material is distributed by the SEI only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

**007 And there is the Copyright Notice.**