IBM Network Protection Advanced Topics

Information

Length:	3.0 Days
__Ref:	IS680G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

Do you need to combat advanced threats? Do you need to protect web applications? This course focuses on advanced configuration and administration of the IBM Network Protection (XGS) appliance. Learn how XGS uses X-Force, PAM, Injection Logic Engine, and other tools to prevent attacks. You also learn how to use APIs to interact with the appliance, implement SNMP, set up a high availability configuration, and migrate policies from the IBM Network IPS appliance to XGS. Troubleshooting techniques are also taught.

Public

This course is designed for security administrators, security analysts, security technical architects, offense managers, network administrators, professional services using IPS solutions, and IPS administrators.

Prerequisits

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- Basic experience with the WMware environment
- TCP/IP networking
- Experience navigating and using the Network Protection local management interface

Before attending this course, you should be proficient in using the Network Protection local management interface or attend IBM Security Network Protection Administration and Configuration (IS671G).

Objective

- Describe how IBM X-Force, the Protocol Analysis Module, and eXpress updates can help prevent attacks
- Use the Injection Logic Engine to prevent SQL Injection and cross-site scripting attacks

- Compare how the appliance can address security issues listed in the Open Web Application Security Project (OWASP) Top 10 report
- Describe the phases of an advanced persistent threat attack
- Provide a high-level description of advanced persistent threat attacks that gained media attention
- Describe how the Network Protection applicance can protect against mutated attacks
- Manage the appliance using application programming interfaces (APIs)
- Configure SNMP alerts generated by response objects and system alerts
- Use a variety of processes, files, and tools to troubleshoot the appliance
- Use the appliance in high-availability networks
- Migrate legacy policies from the Network IPS appliance to the Network Protection appliance

Topics

Unit 1: Protecting against various attacks
Unit 2: Protecting web applications using the PAM Injection Logic Engine (ILE)
Unit 3: Web application protection and the OWASP Top 10 Project
Unit 4: Combating advanced persistent threat attacks
Unit 5: Combating mutated attacks
Unit 6: Using an API to interact with XGS appliances
Unit 7: Implementing SNMP
Unit 8: Troubleshooting techniques
Unit 9: Implementing high availability using XGS
Unit 10: Migrating IBM Network IPS (GX) policies to IBM Network Protection (XGS)