McAfee Network Security Platform (NSP) Administration

Course Content –

Module 1: Welcome

- About the Course
- Acronyms and Terms
- Course Logistics
- Locating Resources on McAfee Business Website
- McAfee Product Training
- McAfee Foundstone Security Education
- ServicePortal
- Security Content Release Notes
- Product Enhancement Request
- Business Community
- Helpful Links
- Classroom Lab Topology

Module 2: Introduction to Network Intrusion Prevention

- Security Threats: The Increasing Risks
- What are Threats and Attacks?
- Common Attack Types
- Motivation and Contributing Factors for Attacks
- Comparing Intrusion Detection and Prevention
- Types of Intrusion Prevention Systems
- Why a Network IPS is Important
- Network Security Platform Overview
- New This Release
- Solution Components
- Attack Detection Framework
- Traffic Normalization
- Ten Steps to Using NSP
- Beyond Intrusion Prevention

Module 3: Planning a McAfee Network Security Platform Deployment

- Choosing a Deployment Option
- Deployment Requirements and Recommendations
- NSM Server Requirements
- NSM Client Requirements
- Windows Display and Browser Settings
- Virtual Server Minimum Requirements
- Virtual Machine Requirements
- NSP 8X Sensor Support
- NSP Server Ports
- Desktop Firewall Requirements
- Using Anti-virus Software with the NSM
- Wireshark
- Single and Central NSM Deployment
- Determining Database Requirements
- Sensor Deployments
- Determining Sensor Placement
  Determining Number of Sensors
- High Availability and Disaster Recovery
- Implementation Process Checklist

Module 4: Getting Started

- Logging into Manager Interface
- Manager Installation Wizard
- Verifying Access to Manager Interface
- Operational Monitors
- Security Monitors
- Navigating Manager Interface
- Managing Dashboard Monitors
- Setting up Basic Features
- Manager Disaster Recovery (MDR) Overview
- Configuring MDR Pair
- Central Manager Overview
- Defining Trust with Central Manager Proxy Server
- Configuring Proxy Server
- IPS Event Notification Overview
- Viewing Summary of IPS Events

- Simple Network Management Protocol (SNMP) Overview
- Configuring SNMP Notification
- Syslog Notification Overview
- Configuring Syslog Notification
- E-mail Server and Notification Overview
- Configuring E-mail Server and Notification
- Configuring Script Notification
- Fault Notification Overview
- Configuring Fault Notification
- Configuring Common Settings for Faults
- Access Events Notification Overview
- User Activity Overview
- Configuring User Activity: SNMP
- Configuring User Activity: Syslog
- Global Threat Intelligence Overview
- GTI Integration Requirements
- Enabling GTI Integration

Module 5: User Management

- User Management Overview
- Minimum Account Configuration
- Role Assignment Overview
- Viewing Roles and Privileges
- Editing the Default Root Admin User
- Adding, Editing, and Deleting Users
- Verifying User Credentials
- Creating a Custom Role
- Assigning Domains and Roles
- Managing My Account
- Managing GUI Access
- Viewing User Activity
- Configuring Banner Text and Image
- Configuring Session Controls
- Configuring Password Controls
- Specifying Audit Settings
- Authentication
- Summary of Authentication Configuration

- LDAP External Authentication
- Configuring LDAP (Up to 4 Servers)
- Assigning LDAP Authentication
- RADIUS External Authentication
- Configuring RADIUS External Authentication
- Assigning RADIUS Authentication

Module 6: Administrative Domains

- Administrative Domains Overview
- Admin Domain's Hierarchical Structure
- How Admin Domains Work
- Managing Admin Domains
- Editing the Root Admin Domain
- Adding a Child Admin Domain
- Adding Users to a Child Domain

Module 7: Network Security Sensor Overview

- M-Series Sensor Portfolio
- NS-Series Sensor Portfolio
- Virtual IPS-series Sensor Portfolio
- Primary Function of Sensor
- Respond
- Inspect
- Classify
- Capture
- Virtualization (Sub-Interfaces)
- Secure Socket Layer (SSL) Decryption
- Acceleration and Operation
- Operating Modes
- Fail-close and Fail-Open (In-line Only)
- Multi-Port Monitoring
- Interface Groups (Port Clustering)
- High Availability
- Large Networks: Perimeter, Core, Internal Placement
- Best Practices

Module 8: Network Security Sensor Overview

- Installing Physical Sensors
- Installing Virtual Sensor
- Managing Sensors
- Devices Page: Global Tab
- Devices Page: Device Tab
- Installing Sensors in Manager
- Establishing Trust
- Downloading Signature Sets
- Reviewing Device Summary
- Viewing/Editing Physical Ports
- Port Types
- Name Resolution
- Network Time Protocol (NTP)
- Proxy Server
- Activity Reports and Logs Review
- CLI Logging
- IPS Event Logging
- Alerting Options
- Remote Access: TACACS+
- Remote Access: NMS Users and Devices
- Customizing Logon Banner
- Special Configurations
- High Availability
- ATD Integration Overview
- DXL Integration Overview
- Maintenance
- Deploying Pending Changes
- Deploying Device Software
- Troubleshooting
- Performance Monitoring

Module 9: Virtualization

- Virtualization (Sub-interfaces) Overview
- Valid interface Types
- Before and After
- VLAN and CIDR Logical Configuration

- Bridge VLAN
- Policy Application
- Determining Direction
- VLAN Tagging
- Double-VLAN Tagging
- CIDR Block Options
- Configuring VLAN Virtual Interface
- Configuring CDIR Virtual Interface
- Configuring Bridge VLAN Virtual Interface
- VLAN Sub-Interface Configuration
- CDIR Sub-Interface Configuration

Module 10: Policies Configuraion

- Intrusion Prevention Overview
- What are Policies?
- Policy Terms and Concepts
- Signatures
- Attack Definitions
- Types IPS Policies
- Policy Assignment
- Inheritance
- How Policies are Applied
- Policy Management Overview
- Adding IPS Policy for Admin Domain
- Copying or Editing IPS Policy for Admin Domain
- Deleting IPS Policy for Admin Domain
- Adding IPS Policy for Interface
- Editing IPS Policy for Interface
- Using IPS Policies Page
- Defining Properties
- Viewing Attack Definitions
- Assigning Policies
- Using Policy Manager
- Interfaces Tab
- Deploying Changes
- Managing Policy Versions
- Deleting Policy

- Policy Import and Export
- Managing Legacy Reconnaissance Policies
- Reconnaissance Attack Settings Merge Utility

Module 11: Policy Customization

- How Attacks Definitions Work
- Traffic Processing and Analysis
- Attack Definitions Tab
- Attack Categories and Severity
- Attack Protection Categories
- Attack Definitions Tab: Customizing Your View
- Attack Definitions Tab: Quick Search, Sort, Columns, Groups, Filters, and Detail
- Attacks Detail Pane: Description
- Benign Trigger Probability (BTP)
- Attacks Detail Pane: Settings Tab
- Managing Policy Groups

Module 12: Threat Explorer

- Analyzing Threats
- Customizing Threat Analyzer View
- Analyzing Source and Destination IP Addresses
- Top Attacks
- Top Attackers
- Top Targets
- Top Applications
- Top Attack Executables
- Top Malware
- Guidelines

Module 13: Advanced Malware Protection

- Advanced Malware Detection Overview
- Malware Engines
- Policy Management Overview
- Advanced Malware Policies Configuration Overview
- Using Advanced Malware Policies Page
- Using Policy Manager
- Malware Policy Parameters

- File Types
- Blacklist/Whitelist Engine
- TIE/GTI File Reputation Engine
- PDF and Flash Analysis Engines
- Gateway Anti-Malware Engine
- ATD Engine
- McAfee Cloud Engine
- Malware Engine Analysis Sequence
- Confidence Level
- Action Thresholds
- Analyzing Malware
- Malware Analysis Overview
- Top Malware Detections Monitor
- Malware Detections Page
- Archiving Malware Files
- Best Practices

Module 14: Advanced Botnet Detection

- Advanced Botnet Detection Overview
- Zero-day and Targeted Botnet Detection
- Heuristics
- Examples of Implemented Heuristics
- Known Botnet Detection
- C&C Server/Callback Detection
- DNS Response Packet Inspection
- Whitelisted and Blacklisted Domains Detection
- Example: Blacklist Domain Detection
- Inspection Options Policies
- How Inspection Option Policies Work
- Policy Management Overview
- Inspection Options Policies Configuration Overview
- Properties Tab
- Inspection Options Tab
- Configuring Traffic Inspection
- Configuring Advanced Botnet Detection
- Advanced Botnet Detection Options
- Legacy Malware Detection Options

- Assigning Policies to Sensor Resources
- Deploying Changes
- Analyzing Botnets
- Top Active Botnets Monitor
- Active Botnets Page: Organization

Module 15: Denial of Service Configuration

- Denial of Service Attacks
- Evolution of DoS Attacks
- Types of DoS Attacks
- Volume-based Attacks
- DoS Learning Mode
- DoS Learning Attacks
- Customizing DoS Learning Attack
- Managing DoS Learning Profiles
- DoS Threshold Mode
- Configuring Thresholds for Volumebased Attacks
- Connection Limiting Policies
- Adding Connection Limiting Policy
- Rate Limiting (QoS Policies)
- QoS and Rate Limiting Configuration Overview
- Adding QoS Policy
- Configuring Rate Limiting Rules
- Protocol Settings
- Configuring Protocol Settings
- Anti-Spoofing
- Stateful TCP Engine
- DNS Protection Command
- Case Studies

Module 16: Endpoint Reputation

- Global Threat Intelligence Review
- IP Reputation
- Policy Management Overview
- IP Reputation Configuration Overview
- Endpoint Reputation Analysis Options
- Deploying Changes

Module 17: Web Server Protection

- Web Server Protection Overview
- How Web Server Heuristic Analysis Works
- Policy Management Overview
- Heuristic Web Application Server Inspection Configuration Overview
- Prerequisite: SSL Decryption
- Private SSL certificates
- Prerequisite: Required Attacks
- Configuring Web Server Heuristic Analysis
- DoS Protection for Web Servers
- Layer 7 DoS Protection for Web Servers
- Web Server – DoS Prevention Configuration Overview
- Configuring Web Server – DoS Prevention
- Assigning Policies to Sensor Resources

Module 18: Firewall Policy Configuration

- Firewall Policy Overview
- Managing Firewall Policies
- Prerequisite: SSL Decryption
- Using Firewall Policies Page
- Using Policy Manager
- Rule Objects Overview
- Adding Rule Object
- Stateless Access Rules
- User-based Access Rules
- Application Identification
- Policy Export and Policy Import
- Firewall Access Logging
- Firewall Access Events
- Firewall Policy Definitions Configuration Report

Module 19: Threat Analyzer

- Threat Analyzer Overview
- Launching Threat Analyzer
- Menu Bar
- Dashboard Page
- NSP Health Dashboard

- Viewing Details for Pie Slice
- Deploying Pending Changes
- IPS Dashboard
- Viewing Details for Pie Slice
- Viewing Attacks Over Time
- Viewing Consolidated Attacks
- NTBA Dashboard
- Applications and GTI View Dashboard
- Adding Dashboards and Monitors
- Customizing the Dashboard Tabs
- Adding a Dashboard
- Adding a Monitor
- Alerts Page
- Viewing Alert Detail
- Managing Alerts
- Right-click Options
- Example Ignore Rule
- Endpoints Page
- Forensics Page
- Preferences Page

Module 20: Policy Tuning

- What is Tuning?
- Why Implement Tuning?
- Prior to Tuning
- Two Phases of Policy Tuning
- False Positives and Noise
- Identifying False Positives
- Steps for Reducing False Positives
- Preventing False Positives
- Start with High-Volume Attacks
- Looking for Patterns
- Preventing Future False Positives
- Disabling Attacks and Alerts
- Adding Low Severity Attacks to Process
- Excessive Alerts
- High-Level Bottom-up Approach

- Analyzing Event
- Sorting by Attack Name
- Case Studies

Module 21: Report Generation

- Reports Overview
- Role Assignment
- Reporting Preferences
- Configuration Reports Overview
- Running Configuration Report
- Next Generation Reports Overview
- Running Default Next Generation Report
- Adding, Duplicating, Editing Next Generation Report
- Traditional Reports Overview
- Running a Traditional Report
- Adding User Defined Report
- Configuring Report Automation
- Viewing Automatically-Generated Reports

Module 22: Operational Status

- Operational Monitors Overview
- Device Summary Monitor
- Manager Summary
- Messages from McAfee Monitor
- Running Tasks Monitor
- System Health Monitor
- Managing Faults
- Viewing Manager Faults from Dashboard
- Viewing Device Faults from Dashboard
- Viewing Faults from Manage Page
- Alert Relevance
- Viewing Alert Relevance
- System Log
- Viewing System Log
- Exporting System Log
- Running Tasks
- Viewing User Activity Log

Module 23: Database Maintenance

- Maintenance Overview
- Archiving Malware Files
- Backing Up Data
- Automating Database Backup
- Viewing Scheduler Detail
- Exporting Backup Files
- Deleting Backup Files
- Database Tuning Overview
- Tuning Now
- Automating Tuning
- Enabling and Defining Alert Pruning
- Calculating Maximum Alert Quantity
- Configuring File and Database Pruning
- Data Archiving
- Archiving Data Now
- Automating Archiving Data
- Export Archives
- Restoring Archive