Troika Firewall
Maestro

Introduction

Firewall is essential design element for enterprise and datacenter security requirements. Organizations are using firewall and other security technologies to secure their perimeter and business critical assets. Ever changing and dynamic business requirement's has ensued complex business interactions hence security has become of paramount interest and topmost priority for organizations to secure the digital information. Firewalls with next generation functionalities and other advance security features prevents sophisticated attacks and ensure authorized access to sensitive information.

TFM has been designed by industry skilled professionals keeping current organization requirements under consideration. Multi-vendor skills with understanding on next generation technologies – application identification, threat prevention- has become key attribute to success of any firewall training program today.

This multi-vendor course helps professionals to understand design aspects of firewall, VPN and threat prevention technologies with hands-on experience on how to design, configure and troubleshoot firewalls, NAT, VPN technologies along with threat prevention strategies to combat advance sophisticated threats.

Prerequisites: CCNA or equivalent certification is desired to attend this course

Technologies covered – Checkpoint firewall, Palo Alto next generation firewall, Wireshark & kali linux

Take away: After completion of this course student will attain understanding on network and security technologies including

- Exposure to multi vendor technologies such as Checkpoint, Paloalto, kali linux and other troubleshooting tools
- Security basics, firewall & other security technologies
    - Packet filter firewall
    - Application gateway firewall
    - Stateful Inspection
    - Next generation firewall
    - Intrusion prevention systems
- Understand and design requirement for enterprise security architecture.
- Stateful and next gen firewall architecture with detailed packet flow.
- Understanding firewall security policy models and attributes.
- Requirement of network address translation
- Security policies enforcement with application identification in next generation firewall

- User based policy enforcement
- Next generation threat prevention
    - Intrusion prevention systems
    - Web filtering
    - Gateway AV
- VPN technologies
    - SSL VPN
    - IPsec VPN
- Designing perimeter with Active-Active and Active-backup cluster
- Troubleshooting firewall with debugs, packet captures , traffic and audit logs

Course content

Module 1 – Firewall Architecture

- Understanding various firewall technologies likes of :
    - Packet filter firewall
    - Application gateway firewall
    - Stateful Inspection
    - Next generation firewall
- Enterprise security architecture – defense in depth / layered security architecture
- Understanding on 3-tier architecture
    - Security Gateway/Firewall
    - Security Management
    - Smart Console tools
- Details about Hardware & flow architecture of next generation firewall
    - Single pass architecture
    - Flow logic
    - Segregated control plane and data plane
    - Hardware architecture
    - Fast path
- Design consideration with firewall security solution
- Detailed Packet flow with Stateful & next generation firewall

Module2 – Network Address Translation

- Overview on NAT requirements
- Network address translation
    - Source NAT
    - Destination NAT
    - Static NAT
    - Dual NAT
    - Persistence NAT , Full con & Half con NAT
- Design consideration while using automatic and manual NAT
    - NAT Specific traffic flow
    - Overlapping network communication using NAT
    - Applications affected by NAT
- Understanding and implementation of NAT policies

Module 3 – Application identification

- Overview of application identification
- Various component & technologies of application identification process
- Application-ID traffic flow
- Overview of security policy
- App-id and security policies configuration
- Advance concepts on application and security policies
    - Application dependencies
    - Managing policy behavior
    - Custom application signatures
- Logging and reporting
- Overview of SSL session setup and underrating of PKI
- configure firewall for SSL visibility
- inbound deep packet inspection of SSL traffic - IPS and other signatures for inbound SSL traffic

Module 4 – User based policies / identity awarenes

- Overview and understanding on user-id
- User-id flow & user based policies
- understanding on user-id process

- Enumerate users and group with Active directory and LDAP
- User id agent identification method
- Captive portal overview for guest authentication

Module 5 –Threat prevention

- Overview of threat prevention modules and security profiles
- Understanding on advance deep packet inspection using
    - Anti-virus profiles
    - Anti-spyware profiles
    - Vulnerability scanning profiles
    - Url filtering profiles
    - File blocking profiles
- Administration of security profiles
- Zone protection profiles

Module 6 – VPN

- Overview of VPN technologies
    - SSL VPN
    - IPsec VPN
- Understanding on policy based vpn and its limitations
- Route based VPN
- Implementing VPN with dynamic routing on firewall
- Understanding on NAT-T in IPSEC VPN
- Advance understanding of mobility requirements and SSL VPN technology
    - Network mode, application mode, thin client
    - Split tunneling , full tunneling
    - End point security

Module 7 – High Availability

- Understanding active-active and active-standby cluster
    - High Availability, load sharing , load balancing
    - Unicast mode
    - Multicast mode
    - Concept of Magic MAC
- Understanding and managing split brain condition

Module 8– Troubleshooting

- Overview of troubleshooting methodology on firewalls
- Troubleshooting of address spoofing issues
- Troubleshooting security policies and NAT
- Checkpoint tools
    - VPN debugging using VPN tools
    - Debugging and maintaining SIC
    - Diagnosing Cluster & logging issues
- Packet level troubleshooting with TCPDUMP
- Troubleshooting using pcap files – overview of wireshark tool
- path and link monitoring configuration to handle failover conditions

Module 9 – centralized management server overview and Deployment

- Introduction to centralized management
- Benefits for using centralized management server in network infrastructure
- Overview of MDM and Panorama architecture

Module 10 – Threat Management/Prevention

- Overview of KALI to Launch Network and application based attacks
- Understanding on Foot printing and Reconnaissance using KALI
- Hacking web application using SQL injection
- Understanding on Denial of Service attacks
- Overview of cyber security best practices
    - File Blocking best practices – Use of Kali to launch attacks
    - URL filtering best practices
    - Vulnerability Protection best practices
    - Traps best practices
- Understanding on reducing attack surface
- Overview on investigating attacks
    - Indicators of Compromise
    - Logs and Reports
    - Log Correlation

Module 11 – Introduction to Ethical Hacking

- Cyber security overview & threat landscape
- Top information security attack vectors
    - Understanding threat vectors
        - Operating systems attacks
        - Application oriented attacks
        - Network level threats
    - Attack lifecycle and phases of attacks
    - Attackers motives
    - Essential terminologies

Module 12 – Introduction to Kali Linux

- Setup virtual environment for Kali Linux and target virtual machines
- Overview of Linux command line
    - Directory structure
    - File permissions
    - User privileges
    - Process and services
- Configuring Networking services on Kali including web server, DNS server etc..
- Managing packages
    - Netcat - The Swiss Army Knife of TCP/IP Connections

Stay Ahead of the curve