7018 South Oak Ave, Dickinson, Texas 77539
Phone: 281-827-2427 website: Globalipv6.com

IPv6 Security Migration

Course Length: 4 Days

Course Description

The IPv6 security course offers hands-on training teaching the latest security issues related to IPv6. You will learn how to recognize and proactively mitigate IPv6 attacks by configuring both IPv6 Access-Control List (ACL) and creating firewall statefull rules. Hands-on labs will be used to re-enforce topics discussed during class. IPv6 hacking tools will be used to actively attack ACL and firewall configurations.

What You'll Learn

- Learn how to write an IPv6 security policy and best practices
- Create ACL and reflexive ACLs to protect your companies network
- Make firewalls IPv6 aware
- Build objects and perform firewall filtering
- Review IPSec filtering and configure IPSec tunnels
- Learn security issues related to IPv6 tunneling
- Discuss and learn to protect against IPv6 extension headers attacks
- Review different recon attacks and exploits within the enterprise network
- Implement security policies on local operating systems and servers
- Configure packet filtering on firewalls and routers

Security Course Topic

Section 1: IPv6 Security Overview

- Hacker Types
- Day zero preparations / prevention
- Assessing your threats
- CIA Triad
- Authentication methods
- 802.1x support
- User authorization
- Cryptographically Generated Addresses (CGA)
- Private Addressing
- Security Overview
- Hacker Types
- Privacy addresses

7018 South Oak Ave, Dickinson, Texas 77539
Phone: 281-827-2427 website: Globalipv6.com

Section 2: Router Access-Control List

- DMZ Layer
- Packet layer
- Packet Filtering
- IPv4 router access-list example
- IPv6 standard access-list
- IPv6 standard access-list example
- IPv6 extended access-list
- Multicast filtering

Section 3: Reflexive ACL Filtering

- ACL overview
  - Named ACLs
  - Standard and Extended
- Reflexive ACLs
- Reflexive configuration examples
- ACL show commands
- Distribute List Example
- Route-Map Example
- Viewing syslog events

Section 4: Operating Systems Firewall

- Windows security overview
- Windows threats
  - XP threats
  - 07 threats
  - Server 2008 threats
  - Microsoft SDI (Server and Domain Isolation)
- Dual-stack host
  - Configuring a dual-stack host
  - Why run dual-stack
  - Dual-stack threats
  - Local firewall configuration
- Linux
  - IPSecconfig and IPSeckey
  - Firestarter, IPCop and Shoreline firewalls
  - Central server control DMVPN (Dynamic Multi-Point Virtual Private Network)
- Local firewall
- Creating custom firewall rules
- Inbound filtering
- Outbound filtering
- Recommended filtering services
- Disabling an IPv6 service
- Netsh firewall show commands
- MAC firewall

Section 5: IPv6 Firewall Configuration

- Supporting a dual-stack firewall
- Inbound and outbound rules

- Creating IPv6 network objects
- Creating IPv6 host objects
- Firewall configuration
- Security issues

Section 6: Hacking Tools and Threats

- Mitigating the hacker probe
- Common hacking tools
- THC IPv6 Attack Suite
- Denial of Service programs
- Packet manipulation
- IPv6 mobility overview
- Home Agent (HA)
- Care of Address (CoA)
- Binding update and acknowledgement
- Security concerns
- Routing header issues
- Reconnaisance

Section 7: Protocol Issues and Threats

- DNS threats
    - Configure a Dual-stack DNS server
    - Deploying IPv6 DNS
    - Security issues running dual-stack DNS
    - IPv6 DNS threats
- DHCPv6 vulnarabilities
- Routing protocols
    - OSPFv3
    - EIGRP
    - RIPng
    - MP-BGP
- Point-to-Point threats

Section 8: Extension Header Threats

- Summary of Address Threats
- Extension Header overview
- Extension address threats
- Extension header order
    - Routing Header Hack
    - Fragment header
    - Authentication header
    - ESP header
    - Destination options
    - Upper layer
- Extension header hacks

7018 South Oak Ave, Dickinson, Texas 77539
Phone: 281-827-2427 website: Globalipv6.com

    - Hop-by-Hop Header hack
    - Routing Header issues
    - Fragmentation Header hacks
    - Destination Option Header duplication
- Scapy6 hacking tool
- Filtering with ACL
- Filtering with firewalls

Section 9: ICMPv6 ND Suite

- Hacker Threats for IPv6
- Neighbor Discovery
- DHCPv6
    - Easy to guess addressing
    - Security concerns
    - Public to public addressing
    - DHCPv6 attack
    - DHCPv6 authentication
- Denial of Service
- Neighbor spoofing attack
- Neighbor cache poisoning
- Man in the middle attack
- Denial of service attack
    - ICMPv6 Attacks
- Anycast threat
- Mitigate Neighbor Discovery threats
- Secure Neighbor Discovery (SEND)

Section 10: Firewalls and IPSec

- Layer 2 firewalls and IPv6
- Layer 3 firewalls and IPv6
- IPSec overview
    - Building a Security Assocation SPD, SAD
    - IKE static key
    - IKE dynamic key
    - Diffie-Helman
    - IPSec Configuration Example
- Site-to-Site
- Authentication methods
- Suggested security steps for remote access
- Secure Neighbor Discovery (SEND)
- Host Denial of Service Hack
- Perfect Forward Secrecy (PFS)
- DAD Attack
- Router Hacks
- Using /127 Serial Links

Section 11: Tunneling Techniques

- 6to4 manual tunneling (IPSec)

  - Sample configuration
  - Static point-to-point
  - Dynamic IGP tunneling
  - 6to4 threats
  - Mitigating 6to4 threats
- GRE tunneling
  - Multipoint GRE 350
- DMVPN (Dynamic Multi-Point Virtual Network)
  - NHRP (Next-Hop Resolution Protocol)
  - NHS (Next-Hop Server)
- ISATAP Tunneling
  - ISATAP threats
  - Mitigating 6to4 threats
- Teredo configuration
  - Teredo threats
  - Mitigate Teredo threats
- SSL VPN

Section 12: IPSec Security

- Explore different tunneling hacks
- Learn how to defend against tunneling issues
- Discuss firewall limitations
- Discuss ACL limitations
- Routing loop attacks using IPv6 tunnels
- Teredo tunneling problem
- Leveraging IPS and Firewall IPS against tunneling

Security LABS

Lab 1: Initial IPv6 Security Lab

- Perform initial IPv6 VLAN configuration on assigned firewall
- Configure IPv6 addressing and routing on assigned router
- Setup host workstation for IPv6 network
- Configure both IPv4 and IPv6 addressing

Lab 2: Standard IPv6 ACL

- Configure standard IPv6 ACL on assigned router
- Test each ACL for proper configuration
- Use show commands to view current configured ACLs

Lab 3: Reflexive IPv6 ACL

- Configured classroom reflexive ACL
- Perform proper filtering for connectivity for HTTP, FTP, SMTP, POP3 and TFTP protocols
- Use show command to verify ACLs are using correct reflexive statefull operation.

Lab 4: Windows local firewall security /application security for IPv6

- Configure local host firewall for filtering network traffic
- Filter specific assigned applications

Lab 5: Configuring IPSec Firewall

- Each student will be required to configured firewall statefull filtering
- Specific filtering rules will be required to configure on each student's firewall

Lab 6: Hacking tools for creating IPv6 hacks

- Configure Scapy6 to craft IPv6 headers and perform classroom hacks
- Use Alive6 for testing classroom firewalls
- Test SourceIPv6
- Use IPv6 probing for address and port number discovery
- Configure and test NMAP

Lab 7: Multicast filter

- Configure firewall to only except specific multicast traffic
- Configure firewall to filter unwanted IPv6 traffic

Lab 8: IPSec 6to4 Tunneling

- Configure 6to4 tunnels
- Test 6to4 tunneling to core network
- Filter unwanted traffic over IPv6 tunneling

Lab 9: DMVPN for IPv6

- Configure Dynamic Multipoint VPN (DMPVN)
- Use show commands to verify proper configuration
- Test DMVPN connection into backbone network

Lab 10: Creating an ISATAP VPN over an ISATAP Tunnel

- Each POD will create an ISATAP VPN over an IPv4 network
- Test ISATAP connectivity by communicating with other students PODs