

IPv6 Security Training - Contents

Author: frank.herberg@switch.ch

Version: 6/2019

Copyright: FIRST Inc.

1. Introduction to IPv6
 - 1.1. Reasons for IPv6
 - 1.2. IPv6 statistics
 - 1.3. IPv4 address situation
 - 1.4. IPv6 Internet Standard (RFC 2460, RFC 8200)
 - 1.5. Network Address Translation
 - 1.6. Main differences IPv4 / IPv6
 - 1.7. A typical IPv6 address
2. Introduction to IPv6 Security
 - 2.1. IPv6 addresses and Security
 - 2.2. Extension Headers and Security
 - 2.3. ICMPv6 and Security
 - 2.4. IPv6 and maturity issues
 - 2.5. New attacks
 - 2.6. Latent threat of IPv6 in IPv4 networks
 - 2.7. Opportunities to improve IT-Security
 - 2.8. Conclusion
3. Local Attacks
 - 3.1. ICMPv6
 - 3.2. ICMPv6 in Wireshark
 - 3.3. ICMPv6 Message Types
 - 3.4. Neighbour Discovery Protocol
 - 3.5. Stateless Address Autoconfiguration SLAAC
 - 3.6. Attacks with Router Advertisements
 - 3.6.1. Rogue Router Advertisements

- 3.6.2. Lifetime 0 Attack
- 3.6.3. Router Advertisement Flooding
- 3.7. Rogue Router Advertisement - Mitigation
 - 3.7.1. Disable IPv6 or RA processing
 - 3.7.2. Mitigation on Switch, RA Guard
 - 3.7.3. Router Preference Parameter
 - 3.7.4. Layer 2 Authentication
 - 3.7.5. Host based filtering
 - 3.7.6. SEND
 - 3.7.7. Deprecation Daemons
 - 3.7.8. Partitioning
 - 3.7.9. DHCPv6 only
- 3.8. Exercise: Rogue RA Mitigation in a real network
- 3.9. Conclusion
- 3.10. Attacks with Neighbor Advertisements
 - 3.10.1. Duplicate Address Detection DOS (DAD-DOS)
 - 3.10.2. Neighbor Discovery Spoofing
 - 3.10.3. Redirect Spoofing
- 3.11. Attacks with Multicast Listener Discovery
- 3.12. Attacks with DHCPv6
- 3.13. Conclusion on Local Protocol Attacks
- 4. Perimeter Security
 - 4.1. Basic IPv6 Firewall Issues
 - 4.2. Firewall Policies in Dual Stack environment
 - 4.3. Recommendations for IPv6 Firewall policies
 - 4.4. Recommendations for filtering ICMPv6
 - 4.5. Remote Neighbor Cache Exhaustion Attack
- 5. IPv6 Extension Headers
 - 5.1. Introduction
 - 5.2. EH and Security
 - 5.3. Fragmentation Issues
- 6. Multicast
- 7. Tunnels
- 8. Reconnaissance
- 9. Network Address Translation and Security

- 9.1. Unique local addresses
- 9.2. Network Prefix Translation (NAT66)
- 9.3. NAT64/DNS64
- 10. Conclusions & the way forward
 - 10.1. How IPv6 affects Security
 - 10.2. Questions to ask yourself
 - 10.3. Recommended IPv6 Security Assessment Tools
 - 10.4. IPv6 Security Lab - Example Setup
 - 10.5. Recommended Resources
 - 10.6. Requirements for (Security) Network Equipment
 - 10.7. IPv6 Excuse Bingo
 - 10.8. CVE entries containing IPv6
 - 10.9. 5 recommendations for a secure IPv6 strategy

Material

250 Training Slides (for 1-1.5 day):

IPv6-Security-Training Part 1

129 Slides, IPv6-Security-Training-Part1-2019.pdf/.pptx

IPv6-Security-Training Part 2

122 Slides, IPv6-Security-Training-Part2-2019.pdf/.pptx

IPv6 Security 101 (for 3-4 hours):

101 Slides, IPv6-Security-101-2019.pdf/.pptx

Virtual Lab Setup

IPv6-Security-Lab.pptx

19 pages Resources for the IPv6 Lab (Students)

IPv6-Security-Lab.docs/.pdf

IPv6 Security Training – Contents (this document)