IPv6 Security Training Course

References

September 2017

Introduction

During the IPv6 Security Course, many references are given, mostly IETF RFCs (Internet Engineering Task Force)(Request For Comments).

This document contain more details about hose references, allowing the course participants to go deeper into details.

In the case of RFCs, information about them, like the date of publication or if it still valid or has been obsoleted or update by another RFC, could be found in the www.rfc-editor.org web site.

Standards References

[RFC2827] P. Ferguson, D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, May 2000, Best Current Practice

[RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, July 2003, Proposed Standard

[RFC3704] F. Baker, P. Savola, “Ingress Filtering for Multihomed Networks”, March 2004, Best Current Practice

[RFC3756] P. Nikander, Ed., J. Kempf, E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats”, May 2004, Informational

[RFC3849] G. Huston, A. Lord, P. Smith, "IPv6 Address Prefix Reserved for Documentation", July 2004

[RFC3971] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, SEcure Neighbor Discovery (SEND), March 2005, Proposed Standard

[RFC3972] T. Aura, “Cryptographically Generated Addresses (CGA)”, March 2005, Proposed Standard

[RFC4191] R. Draves, D. Thaler, “Default Router Preferences and More-Specific Routes”, November 2005, Proposed Standard

[RFC4301] S. Kent, K. Seo, "Security Architecture for the Internet Protocol”, December 2005, Proposed Standard

[RFC4302] S. Kent, “IP Authentication Header”, December 2005, Obsoletes RFC 2402, Proposed Standard

[RFC4303] S. Kent, “IP Encapsulating Security Payload (ESP)”, December 2005, Obsoletes RFC 2406, Proposed Standard

[RFC4443] A. Conta, S. Deering, M. Gupta, Ed., “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, March 2006, Draft Standard

[RFC4541] M. Christensen, K. Kimball, F. Solensky, “Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches”, May 2006, Informational

[RFC4552] M. Gupta, N. Melam, “Authentication/Confidentiality for OSPFv3”, June 2006, Proposed Standard

[RFC4795] B. Aboba, D. Thaler, L. Esibov, “Link-local Multicast Name Resolution (LLMNR)”, January 2007, Informational

[RFC4861] T. Narten, E. Nordmark, W. Simpson, H. Soliman, “Neighbor Discovery for IP version 6 (IPv6)”, September 2007, Draft Standard

[RFC4884] R. Bonica, D. Gan, D. Tappan, C. Pignataro, “Extended ICMP to Support Multi-Part Messages”, April 2007, Proposed Standard

[RFC4890] E. Davies, J. Mohacsi, “Recommendations for Filtering ICMPv6 Messages in Firewalls”, May 2007, Informational

[RFC4941] T. Narten, R. Draves, S. Krishnan, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, September 2007, Draft Standard

[RFC4942] E. Davies, S. Krishnan, P. Savola, “IPv6 Transition/Co-existence Security Considerations”, September 2007, Informational

[RFC5095] J. Abley, P. Savola, G. Neville-Neil, “Deprecation of Type 0 Routing Headers in IPv6”, December 2007, Proposed Standard

[RFC5157] T. Chown, “IPv6 Implications for Network Scanning”, March 2008, Obsoleted by RFC 7707, Informational

[RFC5304] T. Li, R. Atkinson, “IS-IS Cryptographic Authentication”, October 2008, Proposed Standard

[RFC5310] M. Bhatia, V. Manral, T. Li, R. Atkinson, R. White, M. Fanto, “IS-IS Generic Cryptographic Authentication”, February 2009, Proposed Standard

[RFC5722] S. Krishnan, “Handling of Overlapping IPv6 Fragments”, December 2009, Proposed Standard

[RFC5925] A. Mankin, R. Bonica, “The TCP Authentication Option”, J. Touch, June 2010, Proposed Standard

[RFC6052] C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, “IPv6 Addressing of IPv4/IPv6 Translators”, October 2010, Proposed Standard

[RFC6105] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi, “IPv6 Router Advertisement Guard”, February 2011, Informational

[RFC6434] E. Jankiewicz, J. Loughney, T. Narten, “IPv6 Node Requirements”, December 2011, Informational

[RFC6583] I. Gashinsky, J. Jaeggli, W. Kumari, “Operational Neighbor Discovery Problems”, March 2012, Informational

[RFC6666] N. Hilliard, D. Freedman, “A Discard Prefix for IPv6”, August 2012, Informational

[RFC6762] S. Cheshire, M. Krochmal, “Multicast DNS”, February 2013, Proposed Standard

[RFC6763] S. Cheshire, M. Krochmal, “DNS-Based Service Discovery”, February 2013, Proposed Standard

[RFC6946] F. Gont, “Processing of IPv6 "Atomic" Fragments”, May 2013, Proposed Standard

[RFC6980] F. Gont, “Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery”, August 2013, Proposed Standard

[RFC7112] F. Gont, V. Manral, R. Bonica, “Implications of Oversized IPv6 Header Chains”, January 2014, Proposed Standard

[RFC7113] F. Gont, “Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)”, February 2014, Informational

[RFC7123] F. Gont, W. Liu, “Security Implications of IPv6 on IPv4 Networks”, February 2014, Informational

[RFC7136] B. Carpenter, S. Jiang, “Significance of IPv6 Interface Identifiers”, February 2014, Proposed Standard

[RFC7166] M. Bhatia, V. Manral, A. Lindem, “Supporting Authentication Trailer for OSPFv3”, March 2014, Proposed Standard

[RFC7217] F. Gont, “A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)”, April 2014, Proposed Standard

[RFC7610] F. Gont, W. Liu, G. Van de Velde, “DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers”, August 2015, Best Current Practice

[RFC7707] F. Gont, T. Chown, “Network Reconnaissance in IPv6 Networks”, March 2016, Informational

[RFC7721] “Security and Privacy Considerations for IPv6 Address Generation Mechanisms”, A. Cooper, F. Gont, D. Thaler, March 2016, Informational

[RFC8064] F. Gont, A. Cooper, D. Thaler, W. Liu, “Recommendation on Stable IPv6 Interface Identifiers”, February 2017, Proposed Standard

[RFC8200 / STD86] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", July 2017. Internet Standard (Obsoleted RFC 2460)

[RFC8213] B. Volz, Y. Pal, “Security of Messages Exchanged between Servers and Relay Agents”, August 2017, Proposed Standard

Security Tools References

[1] **Wireshark** (www.wireshark.org): Sniffer with a graphical interface that understands a _lot_ of protocols and show them in a user-friendly way. Available for Linux, Windows, and Mac OS. Allows for filtering, and TCP connection follow-up (Follow TCP Stream)

[2] **Nmap** (nmap.org): Network scanner that supports IPv4 and IPv6. Available for Linux, Windows, and Mac OS.

[3] **netsniff-ng toolkit** (netsniff-ng.org): Free Toolkit for Linux, including a sniffer and other tools.

[4] **Macof** (http://www.irongeek.com/i.php?page=backtrack-3-man/macof): Tools that is part of dsniff (monkey.org/~dugsong/dsniff/). It's a MAC random generator that could make a switch's memory to exhaust. Can generate 155,000 MACs in a switch in 1 minute. Some switches when exhaust their memory start acting like a hub.

[5] **Yersinia** (www.yersinia.net): Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. Protocols: STP, CDP, DTP, DHCP, HSRP, IEEE 802.1Q, IEEE 802.1X, ISL y VTP. Para Linux y BSD.

[6] **Ettercap** (ettercap.github.io/ettercap/): Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis. Available for Windows (up to 8), Linux, Mac OS, and BSD. Supports IPv4 and IPv6.

[7] **Loki** (www.ernw.de/research/loki.html): a Python based framework implementing many packet generation and attack modules for Layer 3 protocols, including BGP, LDP, OSPF, VRRP and quite a few others. For Linux and Windows 7.

[8] **THC-IPV6** (www.thc.org/thc-ipv6/): A complete tool set to attack the inherent protocol weaknesses of IPv6 and ICMPv6, and includes an easy to use packet factory library. Available for Linux and BSD.

[9] **Scapy Project** (http://secdev.org/projects/scapy/): Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture

them, match requests and replies, and much more. Runs natively on Linux, and on most Unixes with libpcap, libdnet and their respective python wrapper.

[10] **Chiron** [https://www.secfu.net/tools-scripts/]: An all-in-one IPv6 Pen Testing Framework. It includes enhanced MLD capabilities, DHCPv6 support (both regarding packets and a fake DHCPv6 server), ip(6) tables autoconfiguration at proxy module, etc.

[11] **Pholus** [https://www.secfu.net/tools-scripts/]: An mDNS and DNS-SD security assessment tool, which can be used to create completely custom Queries and Responses, as well as to automate several activities (Reconnaissance, Man in the Middle attacks, Denial of Service attacks using various methods, remote unicast operations, overflow attempts, etc.).

[12] **Topera** (toperaproject.github.io/topera/): Topera is a new security tool for IPv6, with the particularity that their attacks can't be detected by Snort.

[13] **The IPv6 Toolkit** (www.si6networks.com/tools/ipv6toolkit/): Set of IPv6 security assessment and trouble-shooting tools. It can be leveraged to perform security assessments of IPv6 networks, assess the resiliency of IPv6 devices by performing real-world attacks against them, and to trouble-shoot IPv6 networking problems. The tools comprising the toolkit range from packet-crafting tools to send arbitrary Neighbor Discovery packets to the most comprehensive IPv6 network scanning tool out there (our scan6 tool).

[14] **Snort** (www.snort.org): It is an open source intrusion prevention system (IPS) capable of real-time traffic analysis and packet logging.

[15] **Suricata** (suricata-ids.org): Free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing.

[16] **Bro** (www.bro.org): The Bro Network Security Monitor is a powerful network analysis framework that is much different from the typical IDS you may know.

[17] **Nessus** (www.tenable.com/products/nessus): Vulnerability scanner. Free for personal use.