IPv6 Security Training Course

References

March 2022

Introduction

During the IPv6 Security Course, many references are given, mostly IETF RFCs (Internet Engineering Task Force)(Request For Comments). You can also find useful references for RIPE NCC documents, security tools and sources of relevant security information.

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

In the case of RFCs, updated 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.

IETF 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

[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

[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

[RFC7824] S. Krishnan, T. Mrugalski, S. Jiang, "Privacy Considerations for DHCPv6", May 2016, Informational

[RFC7844] C. Huitema, T. Mrugalski, S. Krishnan, "Anonymity Profiles for DHCP Clients", May 2016, Proposed Standard

[RFC8021] F. Gont, W. Liu, T. Anderson, “Generation of IPv6 Atomic Fragments Considered Harmful”, January 2017, 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

[RFC8415] T. Mrugalski, M. Siodelski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon, T. Winters, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, November 2018, Proposed Standard (Obsolotes RFC 3315, RFC 3633, RFC 3736)

[RFC8504 / BCP220] T. Chown, J. Loughney, T. Winters, "IPv6 Node Requirements", January 2019, Best Current Practice (Obsoletes RFC 6434)

[RFC8981] F. Gont, S. Krishnan, T. Narten, R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", February 2021, Obsoletes RFC4941, Standards Track

[RFC9099] É. Vyncke, K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks", August 2021, Informational

RIPE NCC Documents References

[RIPE-554] RIPE-554 "Requirements for IPv6 in ICT Equipment", 4/6/2012 (https://www.ripe.net/publications/docs/ripe-554)

[RIPE-690] RIPE-690 "Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose", 16/10/2017 (https://www.ripe.net/publications/docs/ripe-690)

[RIPE-706] RIPE-706 "Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide", 7/6/2018 (https://www.ripe.net/publications/docs/ripe-706)

[RIPE-772] RIPE-772 "Requirements For IPv6 in ICT Equipment", 14/12/2021, Updates RIPE-554, (https://www.ripe.net/publications/docs/ripe-772)

Security Tools References

[1] **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. Scapy runs natively on Linux, Windows, OSX and on most Unixes.

[2] **Nmap** (nmap.org): Nmap ("Network Mapper") is a free and open source software for network discovery and security auditing. Supports IPv4 and IPv6. Available for Linux, Windows, and Mac OS. It includes the tool Nping for packet generation. It also has NSE (Nmap Scripting Engine) that allows users to write simple scripts, using Lua programming language, to automate a wide variety of networking tasks (see here some IPv6-related scripts that already exist: nmap.org/nsedoc/index.html)

[3] **tcpdump** (www.tcpdump.org): tcpdump is a powerful command-line packet analyzer. Runs on most Unix-like operating systems: Linux, Solaris, FreeBSD, DragonFly BSD, NetBSD, OpenBSD, OpenWrt, macOS, HP-UX 11i, and AIX.

[4] **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).

[5] **Termshark** (termshark.io): Termshark is a terminal user-interface for tshark, inspired by Wireshark. Can capture packets and decode them making it easy to understand their content. Available for Linux, Windows, and Mac OS.

[6] **THC-IPV6** (github.com/vanhauser-thc/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.

[7] **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.

[8] **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 Linux, Mac OS, and BSD. Supports IPv4 and IPv6. Offers three interfaces: command line, GUI and ncurses.

[9] **OpenVAS** (github.com/greenbone/openvas): OpenVAS is a full-featured scan engine that executes a continuously updated and extended feed of Network Vulnerability Tests (NVTs). Originally known as GNessUs, is a software framework of several services and tools offering vulnerability scanning and vulnerability management.

[10] **Snort** (www.snort.org): It is an open source intrusion prevention system (IPS) capable of real-time traffic analysis and packet logging. Has three primary uses: packet sniffer like tcpdump, packet logger - which is useful for network traffic debugging, or a full-blown network IPS. Available for Linux, Windows, and BSD.

[11] **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. Available for Linux, Windows, Mac OS and BSD.

[12] **Zeek** (zeek.org): Zeek is an Open Source Network Security Monitoring tool. It's not an active security device, like a firewall or IPS. Rather, Zeek sits on a “sensor,” that quietly and unobtrusively observes network traffic, interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a SIEM system. Available for Linux, Mac OS and BSD.

[13] **Ostinato** (github.com/pstavirs/ostinato): Ostinato is a network packet crafter and stateless traffic generator that can run on Windows, Linux and Mac OS X. Supports the most common standard protocols and allows to set a value for any field of any to the protocols.

[14] **TRex** (trex-tgn.cisco.com): TRex is an open source, low cost, stateful and stateless traffic generator. Includes support for multiple streams, the ability to change any packet field and provides per stream/group statistics, latency and jitter. Can be installed in Linux.

IPv6 Security Information References

[1] ENISA - European Union Agency for Cybersecurity: https://www.enisa.europa.eu

[2] EUROPOL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[3] European Cybercrime Centre - EC3: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[4] OpenVAS (github.com/greenbone/openvas): is a full-featured scan engine that executes a continuously updated and extended feed of Network Vulnerability Tests (NVTs). It's a software framework of several services and tools offering vulnerability scanning and vulnerability management.

[5] CVE - Common Vulnerabilities and Exposures: https://cve.mitre.org/index.html

[6] NVD - National Vulnerability Database: http://nvd.nist.gov

[7] IETF - Internet Engineering Task Force: www.ietf.org

[8] RFC Editor: https://www.rfc-editor.org

[9] IETF Documents: https://tools.ietf.org/id/

[10] CVSS - Common Vulnerability Scoring System: https://www.first.org/cvss/

[11] Cisco Talos - Disclosed Vulnerability Reports: https://talosintelligence.com/vulnerability_reports#disclosed

[12] IPv6 Hackers List: https://www.ipv6hackers.org

[13] Reddit - Information Security News & Discussion: https://www.reddit.com/r/netsec/

[14] Cisco Talos Intelligence Group Twitter account: https://twitter.com/TalosSecurity

[15] Microsoft - Security Response Twitter account: https://twitter.com/msftsecresponse

[16] Microsoft Technical Security Notifications: https://www.microsoft.com/en-us/msrc/technical-security-notifications

[17] Microsoft Security Update Guide: https://msrc.microsoft.com/update-guide/en-us

[18] SANS Internet Storm Center: https://isc.sans.edu

[19] SANS ISC Twitter account: https://twitter.com/sans_isc

[20] IETF email lists: https://www.ietf.org/how/lists/

[21] NANOG - North American Network Operators' Group mailing lists: https://www.nanog.org/resources/nanog-mailing-lists/

[22] Troopers: https://troopers.de

[23] Black Hat: https://www.blackhat.com

[24] CCC - Chaos Computer Club: https://www.ccc.de/en/

[25] Kaspersky - Vulnerability Report: List of Advisories: https://support.kaspersky.com/general/vulnerability.aspx?el=12430

[26] McAffe - Product Security Bulletins: https://www.mcafee.com/enterprise/en-us/threat-center/product-security-bulletins.html

[27] F-Secure - Advisories: https://labs.f-secure.com/advisories/

[28] Cyber Security Works: https://cybersecurityworks.com/zerodays-vulnerability-list/

[29] Check Point: https://www.checkpoint.com/advisories/

[30] PaloAlto: https://security.paloaltonetworks.com