IPv6 Security Course with Remote Labs - Design and Development

Mr. john pickard, East Carolina University

Instructor Department of Technology Systems East Carolina University

Dr. Te-Shun Chou, East Carolina University
Dr. Philip J Lunsford II P.E., East Carolina University

Dr. Philip Lunsford is an Associate Professor in the Department of Technology Systems at East Carolina University in Greenville, NC. He received a Bachelor of Science in Electricall Engineering and an Masters of Science in Electrical engineering from the Georgia Institute of Technology, and a Ph.D. in Electrical engineering from North Carolina State University. His research interests includee information security, communication technologies, and the cross-discipline application of technologies. Dr. Lunsford is a registered Professional Engineer and a member of ACM, ASEE, and IEEE.

John Spence

IPv6 Security Course with Remote Labs - Design and Development

Abstract

This paper discusses the development of an undergraduate stand-alone course in IPv6 Security to be taught as a special topics course during the upcoming 2013Summer Semester. The course is second in a series developed through an academic partnership with the Nephos6 Academy. Details of the course are reviewed and include course topics, laboratory environment, and certification opportunities for students. The course is designed for online delivery, includes extensive remote-laboratory exercises, and has objectives that align with the IPv6 Forum Certified Security Engineer (Gold) objectives.

Introduction

First defined in January 1995 by RFC1752, the "next generation" IP protocol, IPv6, is the replacement for our current Internet protocol, IPv4. Until recently, it looked as if IPv6 would never become fully adopted and that IPv4, with features such as network address translation (NAT), carrier grade NAT (CGN), and classless inter-domain routing (CIDR), would continue to provide the world with the address space needed. However, this perspective is now changing as organizations and governments have come to realize that IPv4 cannot sustain the future demands of Internet connectivity.

In February 2011, the Internet Address and Naming Authority (IANA) officially ran out of available public IPv4 addresses by issuing the last remaining five /8 blocks of addresses to each of the five Regional Internet Registries (RIRs).[3] In September 2012, RIPE NCC became the second RIR to allocate its final /8 block of IPv4 addresses (APNIC allocated their final block in 2011). Under RIPE NCC's final /8 policy, Local Internet Registries (LIRs) will receive one /22 IPv4 address block, but only if it can prove it really needs the address space, and only if it has purchased an IPv6 address allocation.[9] As the world transitions to IPv6, there will be increased security issues.

Even organizations that have decided IPv6 is not for them cannot ignore it.[4] The fact is that most organizations have hidden IPv6 traffic running across their networks.[14] Organizations are already experiencing growing numbers of IPv6 attacks. Of particular concern are Malware Tunneling in IPv6, Invisible IPv6 Traffic, protocol 41 tunnels (6over4, 6to4, IPv6-in-IPv4, ISATAP, and Tunnel brokers) and Teredo tunneling mechanisms. IPv6 traffic that is being tunneled over IPv4 connections appears to be regular IPv4 traffic, unless security mechanisms are deployed that can inspect it.

Sheila Frankel of the National Institute of Standards and Technology (NIST) says, "The best way for organizations to prepare for IPv6 is to face it head on and decide to do it in the most secure manner possible." She further states, "Now is the time for corporations to start training staff and getting experience with IPv6 so they can protect themselves against IPv6 based attacks.[14]

The need to train IT professionals, especially network engineers, in the use of Internet Protocol version 6 (IPv6) continues to grow as adoption of IPv6 continues to rise.

The Need for IPv6 in Education

A 2010 IPv6 Curricula Studies survey funded by the European Commission found that IPv6 training and studies at universities were not rigorous enough and were not providing students with the IPv6 knowledge or skills necessary to have any critical impact.[8] As a result of this finding, the IPv6 Forum launched the IPv6 Education Certification Logo Program in 2010.[11] The IPv6 Forum encourages colleges and universities to play a key role as part of this program to accelerate the adoption and integration of IPv6 in the Education Curriculum Worldwide. "We believe IPv6 Training will be quite necessary for the whole Internet industry and its users. There is huge demand in China, where IPv6 Internet is now considered as a national strategy", states Liu Dong, Chair China IPv6 Council.[11]

The Importance of Industry Recognized Certification

In May 2012 the IPv6 Forum launched the IPv6 Education Security Certification Logo Program. This program will certify security courses, trainers, and engineers with the Gold Logo Level from IPv6 Forum. Latif Ladid, President of the IPv6 Forum states, "IPv6 security and privacy are going to be implemented again as an after-thought similar to IPv4 simply due to lack of in-depth knowledge in this area. The IPv6 Security Certification Logo program formalizes a concrete curriculum for everyone to benefit from."[10]

Slaman Asadullah, an IPv6 forum Fellow and Co-Chair of the IPv6 Education Certification Program in the United States, endorsed the IPv6 Forum program stating, "Lack of in-depth IPv6 security features and vulnerability knowledge could hamper IPv6 adaption and transition, and also expose current IPv6 networks to higher risks. Understanding the strategic importance of IPv6 security, IPv6 Forum Education Certification has launched this specialty IPv6 security certification program to incubate sound and in-depth IPv6 knowledge."[10]

In 2010 the European Commission assigned the inno Group to conduct a study to identify incentives and best practices that could help efficient and timely deployment of IPv6. One of the findings of the study was the need for a recognized certification scheme that would ensure a minimum level of acquired knowledge and training quality.[12]

Working With An Industry Partner

Working with Nephos6, Inc. and the Nephos6 Academy Program,[15] we developed and delivered an IPv6 Foundations course during the Summer 2012 Semester that prepared students for the IPv6 Forum Certified Engineer (Silver) Exam.[8] The Nephos6 academy program is designed to introduce students to IPv6 and Cloud technologies and equip them with technical skills that complement their chosen fields of study. The partnership with the Nephos6 Academy was instrumental in the success of the IPv6 Fundamentals course. Feedback from the students at the end of the course indicated a strong demand for more in-depth IPv6 knowledge and labs, specifically in the area of IPv6 Security.

IPv6 Security Course

While there are many examples in the literature of courses developed for a wide variety of network security topics, none were found for IPv6 security that included hands-on labs.[7, 13, 17, 19, 20, 23]

The class is designed as a five week distance-education special topics class that will be delivered during the second term of the 2013 Summer Semester. The course will include online synchronous lecture sessions delivered by the instructor two nights each week using Saba Centra web conferencing software. Through the Centra web interface, students can join the lecture sessions live or view them as a recoding later. Asynchronous presentations will be recorded using Tegrity lecture capture software and posted on a class Blackboard web site for students to review, or to download as a video file or podcast. To facilitate lab exercises, a remote lab environment using NDG Lab NETLAB+ will provide students with 24/7 access to live lab equipment.[16]

Course Prerequisites

To maximize student success in the class and to maximize the learning experience, students must be familiar with IPv6 technology. The prerequisite for the course is IPv6 Forum Silver Engineer certification or equivalent, such as a current CCNA or CCNP ROUTE certification, or successful completion of the IPv6 Fundamentals course.

Course Objectives and Outcomes

The course is designed to give students hands-on skills along with IPv6 security knowledge. The objectives for the course are mapped to the Industry recognized IPv6 Forum Certified Security Engineer (Gold) certification objectives.[10] Students completing the course will meet the following objectives:

- Demonstrate knowledge of security impacts of IPv6 integration and the IPv6 specific aspects of IT security
- Explain the security implications of enabling IPv6 in the network
- Explain the operational aspects of managing an IT environment during the transition to IPv6
- Apply best practices in implementing and operating IPv6 in the environment

Students will acquire knowledge in the following areas:

- The scope of IPv6 security in the IT environment to include: network, applications, management, and policies
- Specific elements of the IPv6 protocol architecture that impacts IT security
- IP version independent and IPv6 specific vulnerabilities and their mitigations
- The appropriate methods for performing IPv6 security assessment of an IT environment
- Current IPv6 security best practices
- Industry standards and requirements for IT security products

Labs implemented in the course are designed to provide the student with the following practical skills:

- Capture malformed IPv6 Packets and identify various threat vectors
- Observe IPv6 based reconnaissance techniques and mitigate against them
- Define and implement best practices for ICMPv6
- Observe and mitigate against ICMPv6 DDOS attacks
- Security controls for IPv6 (ACLs, Policies, etc)
- Observe and mitigate first hop security threats
- Implement control plane protection mechanisms
- Observe and mitigate security threats introduced by transition mechanisms
- Secure IPv6 networking (routing protocols, DNS, and MPLS)
- Configure IPsec for IPv6

Remote Lab environment

Hands-on lab experience for the students was an essential element of this course. In the literature there are numerous examples showing that lab experience plays a critical role in student learning.[1, 2, 18] Because this course is taught completely online, the labs must be either remote equipment or simulation. Literature shows that simulation software can limit student curiosity and experimentation.[6] Therefore, to allow students the fullest possible learning experience and maximum opportunities for experimentation, a remote lab with real equipment is the option chosen.

The remote lab solution for the course is the NETLAB+ server appliance by Network Development Group (NDG).[16] NETLAB+ enables academic institutions to host real physical lab equipment on the Internet for distance learning. NDG currently supports more than twelve courses offered by the Cisco Networking Academy, virtualization programs offered by the VMware IT Academy Program[21], storage courses offered by the EMC Academic Alliance,[5] and IPv6 labs by the Nephos6 Academy.

The NETLAB+ server appliance was purchased from NDG labs and requires an annual maintenance support fee. Cost of the system at the time of writing is $6,995 to $19,995 with an annual fee of $2,395 to $ 2,995, depending on specific product edition[16].

The lab equipment is physically located on the East Carolina University (ECU) campus and is shown in Figure 1. Through the NETLAB+ system, the lab resources could be scheduled, automated, and accessed remotely 24/7 by the students over the Internet through a web browser. Firewall access to TCP Ports 80 for the NETLAB+ web interface and 2201for the remote equipment access are required. Students can schedule lab time on an available "POD" of equipment for any day or time that is not already reserved by another student. At the end of the lab reservation the NETLAB+ server performs the following actions: (1) archives the final device configurations and command logs under the student's account; (2) resets all equipment back to a pre-defined state; and (3) returns any unused time back to the Scheduler for another student to use. Instructors can also join a student lab session synchronously to provide real-time feedback and assessment.

Figure 1. IPv6 Security lab equipment.

Lab topology

The topology used for the labs is shown in Figure 2. The lab consists of three Cisco 1941 routers running an Advanced Enterprise K9 IOS release that are connected on point-to-point serial links, two Windows 7 virtual machines, and five Linux CentOS virtual machines running in VMWare ESXi. The virtual machines were implemented in VMware using ESXi version 4.1 and managed through a VMware vCenter server.[22] The routers and virtual machines connect to the NETLAB+ server appliance through an isolated control network. The control network itself consists of the NETLAB+ server, a Cisco 2950 serving as control switch, and a Cisco 2800 ISR router acting as an access server to provide console access to the lab routers.

Two identical "PODs" are built to support the IPv6 Security course. From previous experience, we have found that a "POD" is required for every 10-12 students in a distance course in order to allow all students with enough lab time without scheduling conflicts.

The topology shown in Figure 2 was specifically designed to match the physical topology of existing "cookie-cutter" Cisco Networking Academy topologies that are supported in the NETLAB+ server appliance.[16] Because of the number of VMs required, this design requires a custom POD design within NETLAB+. However, since the base topology is the same as the default NETLAB+ PODs, the underlying lab and control physical layer topologies do not need to be modified. An academic institution that is currently using NETLAB+ to support Cisco Network Academy courses can implement this topology by modifying any of the following NETLAB+ Topologies: Multi-purpose Academy POD, Cuatro Router POD, and Basic Router POD.[16] For this specific course we are modifying the NETLAB+ Multipurpose Academy POD.[16]

Figure 3 shows the remote lab control plane. The NETLAB+ server is configured with a globally routable static IP on the outside interface facing the Internet and automatically binds 169.254.x.x addresses on the inside interface. Students use the outside interface IP to access the NETLAB+ server web interface on port 80. Remote console access to the lab routers via the access server is achieved through port 2201. A control switch connects the Virtual PCs and Servers on the ESXi host to the router Ethernet interfaces using dynamic VLANs.

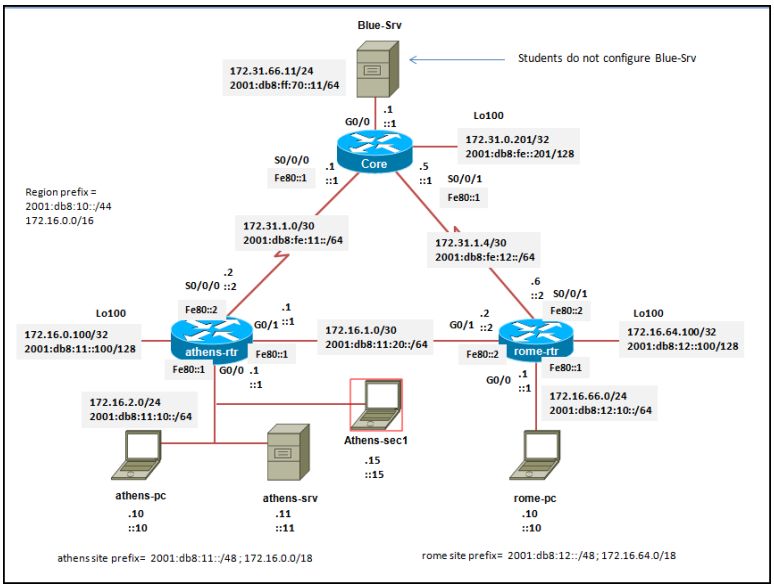

Figure 2. IPv6 Security lab data plane topology.

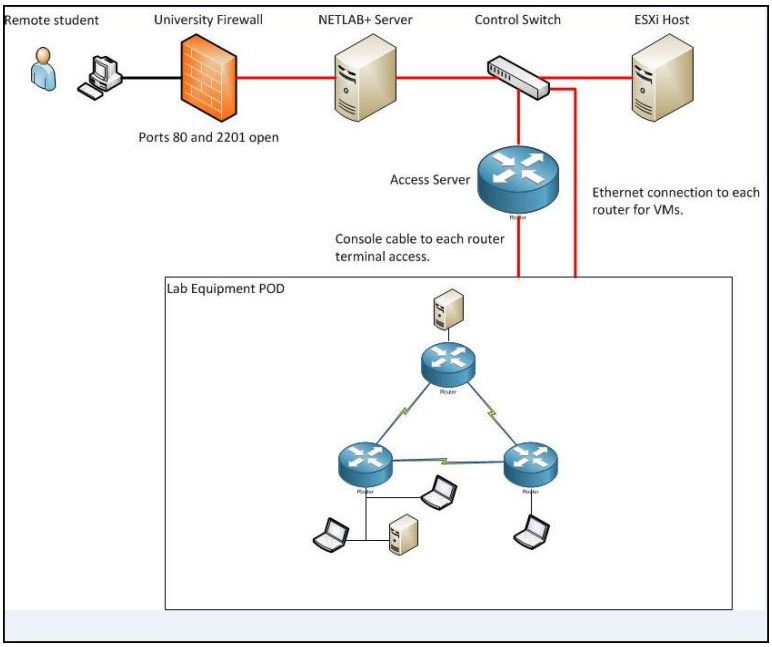

Figure 3. Lab control plane network topology.

Lab Exercise Details

The course includes the twelve labs shown in Table 1. Each lab is designed to take a student approximately one hour to complete. In the labs, students use various tools such as TCPdump running on the Linux host, and Wireshark running on the Windows7 hosts to view and analyze various attack traffic flows.

Lab exercises	IPv6 security concepts
1. Documenting the lab environment	Network documentation
2. On-link discovery using The Hackers Choice (THC) alive6 utility	IPv6 network reconnaissance
3. Using Nmap with IPv6	IPv6 network reconnaissance
4. Introduction to SCAPY	IPv6 packet manipulation
5. Neighbor cache poisoning attack	NDP Vulnerabilities (NS and NA)
6. Malicious DAD responder attack	NDP Vulnerabilities (NS and NA)
7. False redirect attack	NDP Vulnerabilities (RS and RA)
8. Remove default router with forged RA	NDP Vulnerabilities (RS and RA)
9. Off-link prefixes reachable on-link with forged RA	NDP Vulnerabilities (RS and RA)
10. Secure ISATAP deployment	IPv6 transition security
11. Blocking Teredo with RACL	IPv6 transition security
12. Configuring IPsec	IPsec Security

Table 1. Lab exercises and IPv6 security concepts.

Lab 1: Documenting the Lab Environment

Students get an introduction to key tasks that will be performed in all subsequent labs, such as connecting to the end systems, running Wireshark, and accessing the routers. It also gives the students a chance to explore and document the network topology and systems present within the lab environment.

Lab 2: On-link Discovery Using THC alive6 Utility

Students use The Hackers Choice and alive6 to send multicast ping packets with malformed elements onto the network to discover active interfaces that respond with ICMPv6 error message.

Lab 3: Using Nmap with IPv6

Students conduct vertical scans against Windows7 and Linux hosts to discover OS information and to find open ports. Additional tests against the Windows7 Firewall are also conducted.

Lab 4: Introduction to Scapy

This lab provides students with a very brief introduction to the packet generating capabilities of Scapy and then use it to build and send "bogus" packets onto the network.

Lab 5: Neighbor cache Poisoning Attack

Students mount attacks against Windows7 and Linux hosts using The Hackers Choice parasite6 tool to conduct Neighbor Discovery cache poisoning, and false mappings of IPv6 addresses to Layer 2 MAC addresses to set up a Man-in-the-Middle scenario.

Lab 6: Malicious Duplicated Address Detection (DAD) Responder Attack

Students conduct a DoS attack sending malicious Neighbor Discovery (ND) replies to all DAD requests on the network indicating that any requested IPv6 address is already in use. The result is that nodes joining the network cannot configure an IPv6 address, and are therefore, denied access to the link.

Lab 7: False Redirect Attack

Students in this lab use The Hackers Choice redir6 utility and Scapy to manufacture false Redirect packets to become a Man-in-the-Middle spoofing the first hop router. Traffic from the machine under direct attack is routed via the student's attack host, which can monitor packets.

Lab 8: Remove Default Router with Forged RA

The Hackers Choice kill_router6 is used to generate and send forged Router Advertisements (RAs) onto the link. The result is a DoS attack that prevents nodes from communicating with off-link destinations.

Lab 9: Off-link Prefixes Reachable On-link With Forged RA

A Scapy script is used to generate and send forged Router Advertisements onto the local link. The forged RAs cause the Windows and Linux hosts to believe that a distant host is actually on the local link. Traffic intended for the legitimate remote host is instead delivered to the attacker.

Lab 10: Secure ISATAP Deployment

This lab has students configure ISATAP on both a host and on a router; then secure ISATAP access to specific authorized ISATAP clients using an IPv4 ACL.

Lab 11: Blocking Teredo with RACL

Teredo is an automatic IPv6 transition mechanism that is enabled by default on Windows systems, and is running on the Windows7 host in the lab. In this lab, Teredo operations are blocked entirely as they should be in an enterprise scenario.

Lab 12: Configuring IPsec

Students configure IPsec security associations using pre-shared keys, modify default ISAKAMP settings and policies, and create transform-sets on Cisco routers. OSPFv3 authentication with IPsec and redundant IPsec tunnels are also configured.

Conclusions and Future Work

IPv6 has experienced rapid growth in deployment over the last two years, and much of this deployment falls into the category of "unintentional deployment" by virtue that IPv6 is enabled by default on most all enterprise OS platforms. As deployment of IPv6 gains more momentum worldwide, there will be a high demand for those with certified IPv6 skills and knowledge. We strive to help build the pool of IPv6 talent through high quality, certified IPv6 courses.

The IPv6 Security course is the second in a series of three IPv6 courses we plan to deliver at ECU. In summer 2012, we delivered an IPv6 Fundamental course which met with great success. In summer 2013, we will offer both the IPv6 Fundamentals course and the newly developed IPv6 Security course. During the 2013 Summer Semester, we will solicit student feedback on the need for a third course that will cover "advanced" service provider centric IPv6 topics. We will also continue to work with the Nephos6 academy to develop academic curriculum to complement the courses and the lab assignments.

Bibliography

1. Brustoloni, C. 2006 Laboratory Experiments for Network Security Instruction. J. Educ. Resour. Comput. 6(4), 5. doi: 10.1145/1248453.1248458.
2. Cao, X., Y. Wang. Wang, A. Carciula & Wang. 2009. Developing a multifunctional network laboratory for teaching and research. In Proceedings of the 10th ACM conference on SIG-information technology education, 155-160. Fairfax, Virginia, USA: ACM.
3. Curtis, S. 2011. World IPv4 Stocks Finally Run Out. TechWeek Europe.
4. DoD HPC. 2012. IPv6 not Needed Here. Retrieved 11 December, 2012 from http://www.hpcmo.hpc.mil/cms2/
5. EMC. 2012. EMC Academic Alliance. Retrieved 11 December, 2012, from https://education.emc.com/academicalliance.
6. Hamza, M. K., Alhalabi, B., Hsu, S., Larrondo-Petre, M. M., and Marcovitz, D.M. 2003. Remote Labs. Computers in the Schools, 19(3-4), 171-190. Doi: 10.1300/J025v19v03_14.
7. Hartpence, B. 2005. Teaching wireless security for results. In Proceedings of the 6th conference on information technology education, 89-93. Newark, NJ, USA: ACM.
8. IPv6 Forum. IPv6 Education Certification Logo Program. Retrieved 11 December, 2012, from http://www.ipv6forum.com/ipv6_education/.
9. Judge, P. 2012. Providers Pushed to IPv6 as Europe's Last IPv4 Addresses are Issued. Tech Week Europe
10. Ladid, L. 2012. The IPv6 Forum Launches the IPv6 Education Security Certification Logo Program. Retrieved 11 December 2012 from http://www.ipv6forum.com/.
11. Ladid, L. (2010). The IPv6 Forum Launches the IPv6 Education and Certification Logo Program. Retrieved 11 December, 2012, from http://www.gogo6.com/profiles/blogs/the-ipv6-forum-launches-the.
12. Le Gall, F. 2012. Piloting the IPv6 Upgrade for Europe: IPv6 Curricula Study. Inno-group.
13. Liu, C. & B.G. Mackie (2006) Teaching Security Techniques in an E-Commerce Course. Journal of Information Systems Education, 17, 5-10.
14. Marsan, C. 2009. Invisible IPv6 Traffic Poses Serious Network Threat. Network World.
15. Nephos6. Nephos6 Academy Program. Retrieved 11 December, 2012, from www.nephos6.com.

16. Network Development Group. 2012. NETLAB+ Product Overview. Retrieved 1 June, 2012 from http://www.netdevgroup.com/products.
17. Pickard, J., Spence, J., Lunsford, P. 2012. IPv6 Certification and Course Development. Proceedings of the ACM SIGIT/RIIT 2012. Calgary, Alberta.
18. Sarkar, N.I. (2006) Teaching computer networking fundamentals using practical laboratory exercises. Education, IEEE Transactions on, 49, 285-291.
19. Sharma, S.K. & J. Sefchek (2007) Teaching information security courses: A hands-on approach. Computers & Security, 26 290-299.
20. Te-Shun, C. 2011) Development of an intrusion detection and prevention course project using virtualization technology. International Journal of Education & Development using Information & Communication Technology, 7, 46-55.
21. VMWare. 2012. VMware IT Academic Program. Retrieved 11 December, 2012, from http://www.vmware.com/partners/academic/program-overview.html.
22. VMWare. 2012. VMware vCenter Server. Retrieved 1 June, 2012 from http://www.vmware.com/products/vcenter-server/overview.html.
23. Yu, H., W. Liao, X. Yuan & J. Xu (2006) Teaching web security course to practice information assurance. SIGCSE, 38, 12-16.