eForensics Magazine

Computer

VOL.2NO.17

Computer Forensics JumpStart Vol. 3

HOW TO ANALYZE A TRAFFIC CAPTURE

ORACLE LABEL SECURITY

INTRODUCTION TO WINDOWS FORENSICS USING PARABEN P2 COMMANDER

LOGIC BOMBS

STEP-BY-STEP TO ASSESS IT SYSTEM CONTROLS

Issue 17/2013 (21) October ISSN 2300-6986

IPV6 SECURITY SECURING THE FUTURE OF INTERNET

by Satinder Sandhu

Predictions about when the world will end are as consistent as the predictions that when IPv4 internet addresses will finally run out, but some IT security professionals say that it is the least of our worries. A much bigger concern, they say, should be the security holes that will open up in many business organizations as the world moves over to internet protocol version six (IPv6). In this article we are going to discuss and execute the techniques and methodologies which can make the future of internet .... INSECURE!!

What you will learn:

- IPv6 Protocol and Vulnerabilities
- Hands on Network Attacks for IPv6
- Introduction to IPv6 Hacking Toolkit
- IPv6 and Web Assessments
- Exploiting IPv6 using Metasploit
- Security Enhancements in IPv6
- Countermeasures

What you should know:

- You should have a basic understanding of IPv6 fundamentals
- Exposure to TCP/IP Protocol
- Basic knowledge of offensive techniques

The IPv6 Security is an important aspect of the changeover that has been lost in all the hype around how IPv4 is about to run out of IP addresses assigned to each internet-connected device because of the explosion of internet users, devices and web services.IPv6 will solve this problem because it provides over four billion times more addresses than IPv4, but in solving that problem, it could expose businesses to cyber attacks as hackers use IPv6 to bypass security controls, filters designed and configured for IPv4 traffic.

In order to ensure the that we are safe and secure while using the IPv6 network, first we need to know the possible attacks and hacks which can exploit the vulnerabilities of the IPv6. So, in this article we would discuss the techniques, methodologies and tools that make IPv6 ..... insecure.

IPV6 VS OLD ATTACKS

In this section we will analyze some of the most popular cyber attacks in a perspective focused on the comparison and on the possible impact of these with the IPv6.

RECONNAISSANCE ATTACKS

Reconnaissance attacks, in IPv6, are different for two major reasons: The first is that “Ports Scan” and/or “Ping Sweep” are much less effective in IPv6, because of, as already said, the vastness of the subnet into play. The second is

CONCLUSION AND COUNTERMEASURES

Threat	IPv6 Characteristics	Mitigation
Threats with New Considerations in IPv6		
Reconnaissance	Scanning for hosts is not feasible because of large address space. Well-known addresses, in particular multicast, are vulnerable.	Same as IPv4. Privacy extensions can make reconnaissance less effective.
Unauthorized access	End-to-end security reduces the exposure. Extension headers (EH) open new attack venues.	Use privacy extensions to reduce a host's exposure. Use multiple addresses with different scopes. Manage EH use.
Header manipulation	IPv6 can take advantage of chained and large-size EHs. EHs that must be processed by all stacks are particularly useful to an attacker.	The EHs usage should be strictly controlled based on deployed services.
Fragmentation	No fragment overlap should be allowed in IPv6, but some stacks do reassemble overlapping fragments. The impact of tiny fragments is minimal in IPv6.	Use properly implemented stacks that do not allow fragment overlap.
Layer 3/layer 4 spoofing	The use of tunneling offers more spoofing opportunities even though they are not different from IPv4 tunneling.	Same mitigation techniques as with IPv4.

Figure 20. *Mitigation and Countermeasures that can be implemented to ensure IPv6 Security*

CONCLUSION

In the end i would love to suggest you all that as the IPv6 adoption and migration is increasing fast hence the administrator should plan their networks having in mind the security issues, and Industry is in the early stage of IPv6 adoption and for this reason many security breaches didn't appear yet so we need to stay updated. Some good portals for staying updated in the field of IPv6 security and implementation are the following *www.ipv6forum.com* and *www.cisco.com/web/solutions/trends/ipv6/index.html.*

ABOUT THE AUTHOR

Satinder Sandhu is a Cyber Security Researcher and Information Security Consultant currently working for Koenig Solutions Pvt Ltd, India. His main expertise includes Vulnerability Assessment, Network Penetration Testing and Reverse Engineering. He is Computer Science Engineer by qualification and security evangelist by passion!!