XXV Congresso de Iniciação Científica da Unicamp

October 18 to 20 Campinas | Brazil

2017

Study of the “man in the middle” attack in IPv4/IPv6 transition scenario

Matheus Dias Queiroz*, André Leon S. Gradvohl

Abstract

Due to the increasing demand for a more connected world, the need for a transition from the IPv4 protocol to the IPv6 protocol became a current problem. Therefore, the use of transition mechanisms has become inevitable and consequently, the two versions of the protocol will coexist in the network. This scenario implies in legacy security aspects. We reproduced “Man in the middle” attacks in networks with both protocols to identify possible legacy vulnerabilities between IPv4 and IPv6 protocols.

Key words:

Computer networks, Security, Man-in-the-middle attack

Introduction

Due to the increasing demand for a more connected world, the exhaustion of the IPv4 protocol addresses became a problem. A solution for this problem is the use of the new IPv6 protocol.

With increasing traffic of IPv6 in the networks, the studies about its security have become important. Its predecessor, IPv4, presents flaws in its neighborhood discovery mechanism that allows the execution of “man in the middle” attacks.

“Man in the middle” sort of attacks aims at intercepting communication data of one or more hosts, through techniques that direct the data traffic from these hosts to the attacker, without the victims realize it.

Therefore, this study’s goal is to verify if the IPv6’s neighborhood discovery mechanism, implemented at the Neighbor Discovery Protocol (NDP), also presents flaws that allow “man in the middle” attacks.

Another goal of this study is to verify if the studied attacks will have the same result when the network scenario uses the transition mechanisms that allow the coexistence of IPv4 and IPv6 in the same network.

Results and Discussion

The first experiment of this study was the execution of the “man in the middle” attack, exploring the neighborhood mechanism’s flaw of the IPv4. In this case, the protocol used is the Address Resolution Protocol (ARP). We used a technique named ARP Spoofing that consists in sending forged responses from ARP through the attacker, causing its MAC address associated with the IP address of the destination original host.

In this case, we did the attack on the local network. Host A is an FTP client, Host B is an FTP server and the Attacker is just a client within the network, in which the IP addresses are distributed by DHCP through the router. The three hosts are connected to the router LAN port.

The Attacker sends ARP forged responses to the Host A, with its MAC address associated with the IP address of the FTP Server. When the Host A communicates with Host B, it first sends the information to the Attacker and then the Attacker passes it on to the server. This way the Attacker intercepts and analyzes the data and the victims do not realize it.

The second experiment addressed the NDP of IPv6. In this case, there were difficulties by the Attacker in

mapping the network to identify the active hosts. Therefore, we perform the attack using the multicast all-nodes address, where all the active hosts are hit.

Due to the facility of discovering the network gateway, the Attacker sends Neighbor Advertisement packages with the updating address flag as if they were the network gateway, causing that all the hosts update their neighbor cache tables associating the Attacker MAC address to the gateway link-local address.

The result of this approach is that every package that has the external network as the destination, i.e. which is the router WAN network, will be sent to the Attacker. After that, the Attacker will pass on the package to the original gateway, making the attack imperceptible.

The network setting was the following: Host A and Attacker are on the internal network, connected to the router LAN ports and obtained the IPv6 address through the SLAAC setting. Host B is on the external network, connected to the router WAN port, being a part of other network and with IPv6 address manually set.

The roles of each host here are the same as the IPv4 experiment. Besides, in both experiments, the Attacker did not know the network, the number of active hosts and other details of the network topology. Host A used Microsoft Windows 10, Host B used Microsoft Windows 7 and the Attacker used Debian Jessie GNU/Linux.

Conclusions

The neighborhood discovery mechanisms of IPv6, in a similar way of the IPv4 mechanism, demonstrated themselves vulnerable to a “man in the middle” attack. However, we found a great difficulty in performing a mapping of active hosts in an IPv6 network, which makes a local attack more difficult to be accomplished. In future studies, we will verify how these attacks behave in an IPv4/IPv6 transition network.

Acknowledgement

I would like to thank Vice-Provost of Research at UNICAMP for the recognition of this project, and my family for all the support.

ULBRICH, H.C., *Universidade Hacker*. São Paulo: Digerati Books, 2005. 352 p. ISBN 85-89535-95-9.

MOREIRAS, A. M. et al. *Laboratório de IPv6: aprenda na prática usando um emulador de redes / Equipe IPV6.br*. São Paulo: Novatec Editora, 2015. 416 p. ISBN 978-85-7522-418-2