Reconnaissance Attack on IPv6 to IPv4 Tunneling

Nazrulazhar Bahama, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

Anton Satria Prabuwono, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

Teddy Mantoro, Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

ABSTRACT

Internet Protocol version 6 (IPv6) is created to occupy the insufficient current Internet addresses. Consequently this significant contribution offers huge number of Internet addresses. Besides, the security also has been improved to challenge today threats in competent on IPv6 network. As alternative, an automatic tunneling was introduced along with other transition mechanisms to ensure smooth implementation on existing network. However, it’s believed that the implementation of automatic tunneling has altered the form of the IPv4 threats. Then the gained information from this mechanism is exploited to attempt the target network. As a concern, this paper thoroughly describes on potential of reconnaissance attack reach through automatic tunneling named 6to4 Tunneling. The preference development tools and networking defense mechanism suite, is setup to conduct proposed attack method under 6to4 tunnel testbed environment. As a result, the attacking method is feasible to attempt and 6to4 tunnel showed their influence on the achievement of DoS attack in current internet.

Keywords: 6to4 Tunneling, Dual Stack, Internet Protocol Version 6 (IPv6), Protocol Version 4 (IPv4), Protocol-41

INTRODUCTION

IPv6 is a new protocol of internet was developed by Internet Engineering Task Force (IETF) to replace the existing protocol (Raicu & Zeadally, 2003). Initially, the deployments of previous researches were to identify constraints that may occur in IPv6. Throughout years, Transition Mechanism (TM) has been inspired in order to ensure a successful integration of IPv6 into an existing network (AlJaafreh et al., 2008; Narayan & Tauch, 2010). As referred to (Waddington & Fangzhe, 2002), TMs are identified into three main categories based on their operation and the way of their implementation: dual stack mechanisms (Durand, 2001; Hirorai & Yoshifuji, 2006), tunneling mechanisms (Vazao et al., 2004; Waddington & Fangzhe, 2002), and translation mechanisms (Grosse & Lakshman, 2003; Kawarasaki et al., 2003). Among of these mechanism, tunneling is widest implemented nowadays.
IPv6 mandates the inclusion of IP Security (IPsec) (Kent & Atkinson, 1998; Zagar & Grgic, 2006) makes it is more secure than IPv4. Thus, most of threats that dominate the IPv4 network are no longer effective on IPv6 networks (Xinyu et al., 2007). As a result, some of current security issues can be mitigated in the future implementation. However, after a few years of IPv6 services, some of IPv4 threats have been discovered by researchers at the IPv6 environment (Liu et al., 2009). In addition, the researcher in (Bahaman et al., 2011) stated that this automatic tunneling as a reason for the spreader threats without being detected by intrusion detection tools. Even though, it has been acknowledged by (Deering & Hinden, 1998; Savola & Patel, 2004) about this situation, but the only provide a more theoretical approach on their proposed steps.

As a significant, this paper proposes the possible methods of reconnaissance attack through the medium of 6to4 tunneling. The method focuses on silent mode of reconnaissance attacks; to determine which tunneling interfaces within a subnet are alive. Firstly, the possible method of the attack is review and identified. Then, this method is presented in equation form to understand clearly. Here, the testbed was developed in order to acquire the desired environment. Next, the proposed attacks were constructed and triggered through the testbed. The mentioned attack were carried out using a Python platform tool, Scapy (Burns et al., 2007; Hogg & Vyncke, 2009). At same time packet analyzer was appointed as monitoring and validating function.

The following section of this paper will explain the background of tunneling mechanism and DoS threats. The explanation on methods and testing scenario is detailed in the following section. There will be a further discussion on the experiment in the section afterwards. Then we will further discuss the test results. Finally, the conclusion for this research is explained.

RELATED WORK

IPv6 to IPv4 Tunneling

During transition period, by ignoring automatic tunneling when defining network security policy, will cause any possible unauthorized traffic pass through the network security devices through tunnels. Similarly, the issue wills also occurred with file sharing applications using TCP port 80 globally with IPv4. As noted in (Hanumanthappa & Manjaiah, 2009; Savola & Patel, 2004), automatic tunneling mechanisms are susceptible to packet forgery that refer to DoS attacks. More horrifying, these threats are the same as in IPv4, but larger on the number of paths of exploitation. In addition, relay technologies also was introduce in automatic tunneling with application of DoS vectors. These risks have no difference as IPv4, but emerged new avenues for exploitation (Savola & Patel, 2004).

In this study, the investigation is covered specifically on an automatic 6to4 tunneling as TM due to security issues. Here, 6to4 which is one of tunnel technology is preferred to grant unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. It encapsulate IPv6 packet as IPv4 payload and used protocol number neither 6 (TCP) nor 17 (UDP) but 41(Protocol-41) in protocol field of the IPv4 header. The 6to4 assume that entire IPv4 Internet as a link. The simplest implementation of 6to4 is applied between multiple networks. The task is done by connected each of them with IPv4 Internet connection which may a corporate network or the global Internet.

Major requirement is to send protocol-41 packet to another via any type of networks. At the end of 6to4 tunnel consists of a 6to4 Host/Router, 6to4 Router, or 6to4 Relay Router. Once configuration of 6to4 tunnels done at any interface the router, it will be called 6to4 router. If the configuration is added and then be able to communicate with the IPv6 internet, it
Resource Allocation for Multi Access MIMO Systems
www.igi-global.com/chapter/resource-allocation-multi-access-mimo/70818?camid=4v1a