[Optional] IPv6 Firewalls

COSC301 Laboratory Manual

Old Lab

This lab hasn't been run recently, so no guarantees are made regarding the commands and their output.

The format of this lab is more like a self-guided tutorial. Part of the difficulty of learning about firewalls is now how to implement the rules, which we have done in the previous firewall lab, but rather figuring out what sorts of attacks you need to defeat.

The basic attacks don’t really change much between IPv4 and IPv6, so this tutorial applies to both. IPv6 does have some extra cautions, mostly because of tunnelling, but that is also present in IPv4 as well.

One of the things that is often a target for firewalling is ICMP and ICMPv6. However, care needs to be taken, especially with ICMPv6, as you can easily break communication when filtering the Internetwork *Control* Message Protocol (for v4 or v6). So some of this tutorial will be spent looking at the suggested best practices in this regard.

By the end of this tutorial, you should have a good idea of some of the types of attacks experienced today, and what sorts of ICMP and ICMPv6 traffic should be able to make it through your firewalls. You should also be able to develop an understanding of common limitations in firewalls.

1. Research and briefly describe the following sets of terms (the list is certainly not exhaustive). Where multiple terms are listed, you should be able to explain what is similar about the terms in each group, as well as be able to explain what is different.

1. Ingress filtering, Egress filtering
2. IP Spoofing
3. Directed broadcast, Backscatter
4. Smurf attack, Fraggle attack
5. BotNet
6. Denial of Service (DoS), Distributed Denial of Service (DDoS)
7. SYN flood, Ping of death
8. Source routing (IPv4 and IPv6)
9. ARP Poisoning, (IPv6) Neighbour Discovery attacks.
10. Connection hijacking, session hijacking.
11. Deep Packet Inspection (DPI) aka Layer 7 filtering, [Network] Intrustion Prevention System (IPS).
12. 6-in-4 tunnel aka Protocol 41 tunnel, 6to4, Toredo, IPSec ESP, VPN, Covert tunnel.

2. Summarise RFC 2827 “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, briefly describing how ICMP should be handled by a firewall.

(To make it easier on yourself, you do not need to consider the issue of multihomed networks).

3. Summarise RFC 4890 “Recommendations for Filtering ICMPv6 Messages in Firewalls”, briefly describing what should be allowed through a firewall.