LAB12B: Ping of death

[Simon X. Camilo. Cybersecurity Student]

[BHCC CIT-275-WB Professor Philip Kazanjian]

Introduction

This document will show a ping of death created through scapy, this is an attack that tries to crash a target, and it will then show how this attack can be detected by using the IDS, Snort.

## What is Scapy?

Scapy is a powerful packet manipulation program that performs better compared to many other tools. This tool can be used to perform a DoS attack on a server, and also slip by the firewall rules set in the server. (Scapy.net, 5/9/2018)

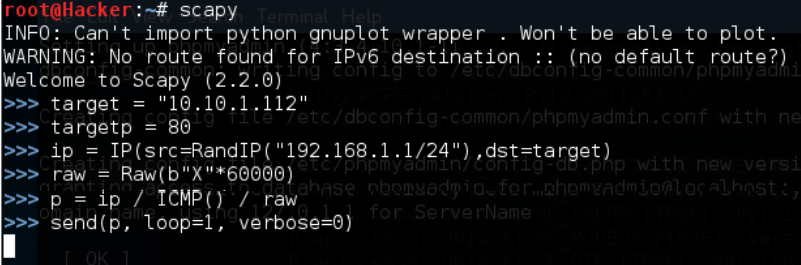
## What is an IDS?

IDS stands for Intrusion Detection System. These systems monitor traffic coming through a server or device, and it reports activities that are considered suspicious by the network administrators. The administrators usually give rules to the IDS (snort in this case), if there is a match they will know about the suspicious activity, but Snort won’t take any action against it.

# Analysis

## **Making a Ping of Death attack**

There are many ways to create a DoS script for Scapy. The script I used is show in image 1

  
**Image 1**

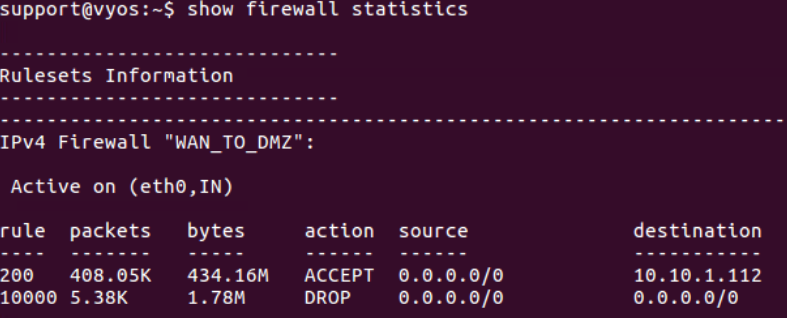
*Scapy DoS ping of death script*

This script sends many icmp packets filled with “X’s” to the target’s (“10.10.1.112”) port 80, while at the same time making the packet show a different source ip address for each packet, making it harder for the attack to detect and also to be stopped by the firewall anti-DoS systems. Using scapy is very simple, and the script is also very simple to do, the script is going to be deconstructed below to show how an attacker might try to attack the systems

* target - The ip address of the target for DoS
* Targetp - The port that the packets are going to use to enter in the target’s machine
* ip = IP(src=RandIP(“192.168.1.1/24”), dst=target) – creates ip packet
  + RandIP - this packet will say where the packet comes from, which will be a random ip address that will hide the identity of the attacker and make these packets harder to ignore.
  + Dst=target - This packet also has the ip of the target
* ICMP - Tells Scapy to use the ICMP protocol, this is the protocol used to ping devices or see if they are online.
* raw = Raw(b”X”\*(60000) – Data of the packet. The packet size is large to consume more resources from the network
* p = ip / ICMP / raw – puts all the layers in one variable. This creates the payload
* send(p, loop=1, verbose=0) – Executes the attack, loop will make the packet not stop sending until the attacker makes it stop.

(Am0nt31r0, 9/30/2018) (Pierre, 8/4/2017)

As shown in image 2, firewall has accepted over 400k packets through the firewall, this means that the attack was succesful.

  
**Image 2**

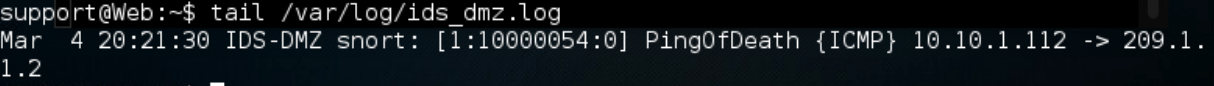
*packets are being accepted through the stateful firewall*

## **Detecting a ping of death DoS attack with Snort.**

To make an alert that will alert the system administrators when there is a ping of death attack against the systems. The first thing to take in mind is that the average inoffensive icmp packets are usually a maximum of 76 bytes in size according to Chris Partsenidis from Firewall.cx, this means that any packet higher than 76 could potentially be a ping of death attack. Because of this, every icmp packet that’s bigger than 80 (just in case) will be detected and reported by Snort. Below is the rule that has been entered into Snort’s configuration file

alert icmp any any → any any \ (msg:”Potential Ping of Death attack”; sid: 10000054; dsize: >80;)

Image 2 shows that Snort is alerting the system of an attempt at a ping of death attack after it has detected it.

  
**Image 3**

*Snort detects a Ping of Death attack and sends an alert.*

(Simon1207, 6/30/2017) / (Partsenidis, 9/30/2018) / (Cisco Community, 11/24/2011)

# Conclusion

Scapy is a very advanced tool that gives attackers a lot of control to attackers, sometimes the business may not have the tools necessary to stop these attacks but detecting these attacks is affordable and not complicated. Snort is a tool that has proven to be very decent in detecting lethal attacks such as a ping of death, which will allow administrators to take action as soon as possible.

References

Philippe Biondi and the Scapy community. (2018, May 9). Scapy. Retrieved March 03, 2021, from <https://scapy.net/>

Philippe Biondi and the Scapy community. (2016, August 3). Usage¶. Retrieved March 03, 2021, from <https://scapy.readthedocs.io/en/latest/usage.html>

Pierre. (2017, August 04). Scapy - persistent randip. Retrieved March 03, 2021, from <https://stackoverflow.com/questions/45509493/scapy-persistent-randip>

Am0nt31r0. (2018, September 30). Am0nt31r0/ping-of-death. Retrieved March 04, 2021, from https://github.com/am0nt31r0/Ping-of-Death/blob/master/pingOfDeath.py

Partsenidis, C. (2004, June 30). What are the minimum and maximum sizes of an icmp packet? Retrieved March 04, 2021, from https://searchnetworking.techtarget.com/answer/What-are-the-minimum-and-maximum-sizes-of-an-ICMP-packet

Cisco Community. (2011, November 24). Icmp packet size? Retrieved March 04, 2021, from https://community.cisco.com/t5/switching/icmp-packet-size/td-p/1818357

Simon1207. (2017, June 30). Simon1207/snort-rules. Retrieved March 04, 2021, from <https://github.com/Simon1207/Snort-Rules/blob/master/local.rules>