LAB11B: Scapy against a stateful firewall

[Simon X. Camilo. Cybersecurity Student]

[Redacted]

Introduction

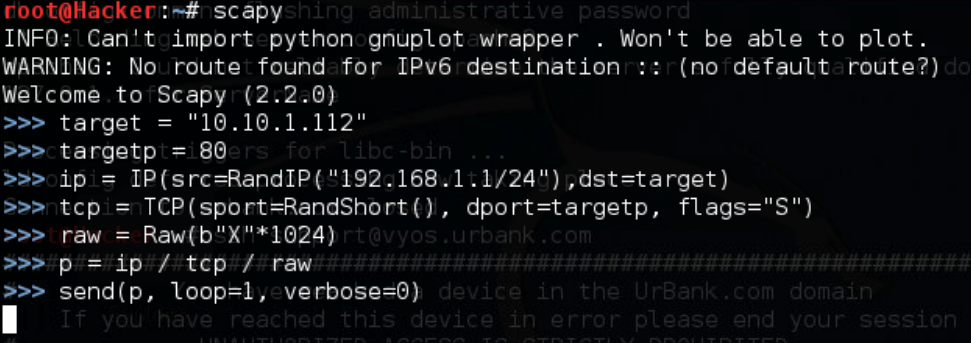
This document shows an attempt at creating a DoS attack that will bypass a stateful firewall using Scapy. Scapy is a powerful packet manipulation program that performs better compared to many other tools. This tool can be used to perform a DoS attack on a server, and also slip by the firewall rules set in the server. This document also has a strong focus in figuring out and researching ways to prevent these attacks from happening.

(Scapy.net, 9/5/2018)

# Analysis

## The DoS attack

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

  
**Image 1**

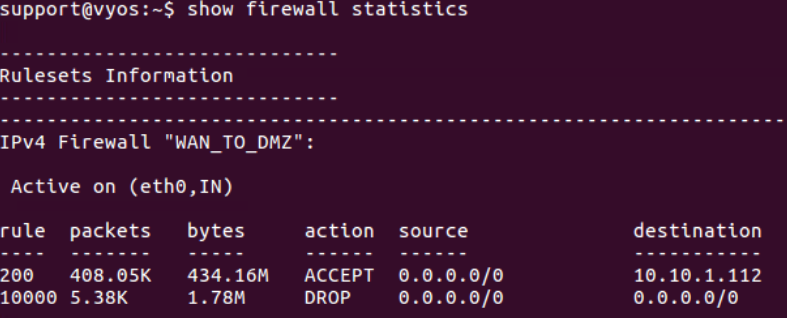
*Scapy DoS script*

This script sends many SYN ack 1kb 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
* tcp = TCP(sport=RandShort(), dport=targetp, flags=”S”) – Creates tcp SYN packet
  + sport =RandShort() – sets the source port for the tcp packet, RandShort will make it choose random ports so the attacker is harder to detect and stop
  + dport=targetp – sets the port of the target
  + flags=”S” – It sets the flag of the tcp packet, which in this case is S, meaning SYN packets
* raw = Raw(b”X”\*(1024) – Data of the packet
* p = ip / tcp/ 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.

(Rockiz, 9/8/2020) (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. This won’t make the site go down since more machines are needed to make the site crash.

  
**Image 2**

*packets are being accepted through the stateful firewall*

## **Preventing this DoS**

The way to bypass a SYN DoS attack of this kind, is to use SYN cookies. SYN cookies will allow the website to keep working even if the SYN queue is filled. This method works by creating a 32-bit encrypted cookie that is sent to the attacker, this cookie contains information needed to generate the “initial sequence number” which expires in 4 seconds. An attacker won’t have enough time to bypass this key attack. Once the time expires, the packets from the attacker are ignored, and there is no way to decrypt this cookie through command prompt, without revealing who the true attacker is.

(Lemon, 4/12/2001)

# Conclusion

Scapy is a very advanced tool that gives attackers a lot of control to attackers, but it will often times not be enough, when filling the SYN queue is no longer an avenue an attacker can use to attack a website. When SYN Cookie is used, attackers will try to take away bandwidth from the servers in order to minimize the availability of the server, this is why botnets had become so popular and expensive. As of today, no measure had been efficient a DoS attack done by a botnet.

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

Rockikz, A. (2020, August 09). How to make a syn flooding attack in python. Retrieved March 03, 2021, from https://www.thepythoncode.com/article/syn-flooding-attack-using-scapy-in-python

Lemon, J. (2001, December 04). Syn cookies. Retrieved March 04, 2021, from <https://www.usenix.org/legacy/publications/library/proceedings/bsdcon02/full_papers/lemon/lemon_html/node9.html>