|  |
| --- |
|  |
| Capstone ExperienceIST 894 |
| Lab 5 – Denial of Service AttacksScott Finlon |

Table of Contents

[1. General Context 3](#_Toc84601426)

[2. Technical Context 4](#_Toc84601427)

[3. Solution 5](#_Toc84601428)

[References 10](#_Toc84601429)

# General Context

In this lab we use a software application called Metasploit to cause a Denial of Service (DoS) attack against a Windows endpoint. A DoS attack is an attack that is meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding a target with traffic, or sending information that triggers a crash (What Is a Denial of Service Attack (DoS) ?, n.d.). Information Security focuses it’s goals and objective around the ‘CIA triad’ which stands for Confidentiality, Availability, and Integrity. These three principals form the cornerstone of any organizations security infrastructure, posture, and policy (Walkowski, 2019).

What this means is that it can be somewhat tough for Information Security professionals to know that they are succeeding at their jobs. It’s not possible to know how many attacks and threats you may have stopped, but it is possible to know that you’ve ensured the confidentiality, integrity, and availability of a system, message, data stream, application, or other. DoS attacks take direct aim at the principal of availability, so it’s crucial that as Information Security professionals we are prepared to prevent the many different ways that different systems can be attacked.

DoS attacks can come in many different attack styles. If a web service only has a set number of connections available or memory or other resources, it’s somewhat simple to launch an attack to exhaust all available resources and if the attack is using everything that’s available nothing is left for normal users. Resource and connection exhaustion happens because of how TCP works. TCP has a three-way handshake that consists of a SYN, an ACK, and then a SYN-ACK, and if an endpoint sends a SYN packet the service will wait until the set timeout period before releasing the connection. This means that an attacked can send a ‘SYN-flood’ that just sends massive amounts of SYN packets and then nothing else which ties up all of the connections until they time out. SYN floods are described in much greater detail in Cloudflares page on ‘How does a SYN flood attack work?’ (SYN Flood DDoS Attack, n.d.). The biggest difference between a SYN flood attack and a DoS attack against a vulnerable system, is that SYN floods can work against systems that are fully patched and don’t have any exploitable vulnerabilities one of the best ways to prevent these attacks are with an additional piece of hardware like a SYN-proxy, there are third party services like Cloudflare that can handle the initial TCP handshake and not forward the connection on to your services until it’s completed which reduces the load on your services to only be full-fledged connections, but they can also be mitigated by increasing the total number of connections allowed as well as reducing the timeout limit so stale connections get terminated more quickly. Other DoS attacks most often work because certain applications and hardware have different vulnerabilities in them that react poorly when presented with a certain specialized packet of data, so sometimes attackers will identify these weaker systems or applications and launch various ‘bad packets’ to try to crash their target rendering them unavailable. The DoS of choice for many attackers in recent years is a Distributed Denial of Service where thousands upon thousands of endpoints in different botnets all send traffic at a specific target overwhelming the target and even the internet connections for it making it so no legitimate traffic can get in or out. In this lab, we are focusing on the second example. We will be identifying our target, and seeing Remote Desktop running we can load up a RDP exploit and launch our attack.

# Technical Context

Back in my undergrad course work I was told “if you’re going to defend your network from hackers, you have to think like one”. That is the basic intention of this lab. We fire up a Kali Linux virtual machine, as well as a vulnerable, exploitable Windows 7 virtual machine. The goal of the lab is started at the onset, but we know we have a machine with an arsenal of penetration testing tools, and we have a vulnerable machine that we are meant to DoS, but how?

One of the first things that any attacker will do is look to see what is on the localized network to give them a chance to move laterally. Crowdstrike says that there are three stages to lateral movement: reconnaissance, credential/privilege gathering, and gaining access to other computers on the network (Lateral Movement Explained | What Is Lateral Movement?, n.d.). In this lab, we aren’t trying to gather credentials or gain access, but the reconnaissance is the important part. We have it easy because we are on the Windows machine so we can just executre `ipconfig` and see it’s IP address, as a true attacker we would need to identify the network and subnet size that the compromised machine is on, and then perform a scan looking for alive hosts, followed by a scan to see what ports are open on those hosts that were found. When we scan our Windows VM we see that port 3389 is open in listening, which is the registered port for Microsoft Remote Desktop Protocol (RDP). RDP has a lot of vulnerabilities and overall weaknesses so it should always be protected and not directly exposed to the internet, but in our case we’re already on the internal network. Rather than try to exploit the RDP service to gain access to the machine, it’s our mission to just find and execute a DoS on the machine to prevent others from being able to use it.

This is a good introduction to some basic functionality of how Metasploit and Nmap function, but most attackers wouldn’t find their way to access on an internal network only to do something that was a noisy as a DoS to bring unwanted attention to them. So while educational, it’s not exactly realistic example of what an attacker in the real-world would actually do.

# Solution

**We start of this lab by starting up both the Kali Linux and Vulnerable Windows VMs. The next step is to log on to the Windows machine, open a command prompt, and then run `ipconfig` which will give us the IP address of the target that we will be attacking.**

****

Figure 1 - start up both virtual machines



Figure 2 - identify the Windows VM IP address

 **The next step is to switch over the Kali Linux box and start up Nmap to scan the Windows host looking for open ports by running the command `nmap -p- 10.1.112.145` where the -p- tells Nmap to scan all 65,535 ports. In Figure 3, we can see the Nmap results showing port 3389 open, but it also shows 999 filtered ports.**



Figure 3 - Nmap scan results

 **If we modify the Nmap command slightly we can change the scan type, and also enable debug which will give us some additional information about the filtered ports. Nmap will put ‘filtered’ when it cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. In Figure 4, it shows that the 999 ports were filtered because they were ‘no-responses’.**



Figure 4 - Nmap debug output

 Now that we know that 3389 is open, we can first start up the PostgreSQL service on our Kali Linux box, and then start up Metasploit with `msfconsole`. Then we search for an appropriate module. We know we are targeting RDP on Windows and we want to DoS it, so search for `dos/windows/rdp’ and ‘auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids’ shows up as a ‘Microsoft Remote Desktop Use-After-Free DoS’ module.

**

Figure 5 - Start PostgreSQL

**

Figure 6 - Search in Metasploit

 We use the `use` command in Metasploit to select that module, and then set our remote host or rhost as the IP of the Windows vulnerable machine. We can run `show options` to verify the module and rhost and rport, and then finally run `exploit` to start the attack.

**

Figure 7 - Metaploit Module Options

**

Figure 8 - Launch Attack From Metasploit

 Finally, if we switch back to the window for our vulnerable Windows host, you’ll see an error pop up that the Windows machine is no longer available because Metasploit sent a corrupt packet to port 3389.

**

Figure 9 - Windows No Longer Accessible

# ****References****

*Lateral Movement Explained | What is Lateral Movement?* (n.d.). Crowdstrike.Com. Retrieved October 7, 2021, from <https://www.crowdstrike.com/cybersecurity-101/lateral-movement/>

*SYN flood DDoS attack*. (n.d.). Cloudflare. Retrieved October 6, 2021, from <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>

Walkowski, D. (2019, July 9). *What Is The CIA Triad?* F5 Labs. <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>

*What is a denial of service attack (DoS) ?* (n.d.). Palo Alto Networks. Retrieved October 7, 2021, from <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>