CA645 Network Security Assignment

Introduction
In the video, we filmed an IP spoofing to DOS, an HTTP server. This attack has advantages and drawbacks.
First the advantages:

- We are anonym
- We don’t receive any response from the server
- Simple to implement.

Then the disadvantages:

- It’s a blind attack we are not sure of what is happening once sent.
- The failure is easy to secure.
- Take all resources available on your pc to flood.
- Once the flood stops the server is available once again.

Explanation of attack

We could be going further in our attack. Here we spoof a random IP address (200.200.200.20) but we can also DOS a target using the server responses that will flood the IP address we used. Here in our example, we could replace it with 10.0.0.2 to flood the second with TCP answers VM.
This failure implies that many other attacks could be implemented. Blind attacks such as TCP Blind In-window Attacks (A user is connected to a server using TCP. We could as an attacker be asking for reset operation on the port hoping to guess the right port and renew the connection and be connected as the previous user session.)

Prevention

The solution we implemented works fine but it doesn't avoid DOS if we use the original IP address. Moreover, the solution isn’t scalable because for each new IP that wants to contact the server we have to add the IP manually. Another solution could be to implement a fail-to-ban on the server. If the user makes too many requests or fails to connect 3 times in a row we ban the IP (here as we use a cisco router as a server I don’t think it’s possible).

Tools Used

1. **Hping3:** It is a Linux utility that is used to create custom packets and also provides the functionality of flooding on specified ports.
2. **Kali Linux:** this distribution of Linux is used by the pen-testers to take a look at the vulnerabilities inside an application or a network. It contains a lot of tools that may be used for discovery and analysis. For example, Metasploit is available on Kali Linux, if we scan the server using this tool we may discover some vulnerabilities that are present inside the setup of our server.

Conclusion
Even though there is a lot of processing power available these days and tons of servers, these kinds of attacks are still in the market. It's easy and an attacker can create bots and flood any server possible. So, it's better to take basic security measures rather than relying

on processing power and mirror servers. To conclude, these attacks may not be a big threat to information integrity or authentication but the loss of availability for a second can cause big financial damage.