1. What is the attack? Why do you want to experiment?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up a highway, preventing regular traffic from arriving at its desired destination.

2. Step by step of how you set up the environment

Server:

1. In the Server Manager, go to the Dashboard section.
2. Select Add roles and features.
    a. Select Role-based or feature-based installation.
    b. Select your server in the list.
    c. Select Active Directory Domain Services.
    d. Click through until you start the installation and then keep the wizard open as it installs everything.
3. Click the link to Promote this server to a domain controller.
4. Go through the AD DS Installation Wizard:
    a. Select Add a new forest.
    b. Set the Root domain name to be: comp3550.private
    c. For the Forest functional level and Domain functional level, choose Windows Server 2012 R2 or Windows Server 2016, depending on which version of Windows Server you're using.
    d. Choose a password for the Directory Services Restore Mode account.

e. Ignore the warning about DNS delegation.

f. Don't change the NetBIOS domain name.

g. Select the default locations for the various folders

h. After it runs prerequisite checks, click Install.

5. After installation is complete (takes ~5 minutes) the server will reboot.

3. Step by step of how you conducted the attack. Elaborate on all the numbers you see during the attack (network traffic, etc)

- The script pulls information from libraries and creates a connection to the network
- Once connected to the network, the attack script then obtains the client IP address and connects. Once connected, the attack begins
- In the attack, packets are flooded to the client machine through the IP address
- For our attack, we send on average 32,480 packets in order to bog down the system and prevent use of the machine.
    - In a real attack, we would send a lot more packets, but for the sake of time and resources, we had to scale.
- This attack is then mitigated and the connection to the attacker is broken

4. Analyze the impact on the network/honeypot/users

A ddos attack makes accessing the machine being attacked almost impossible, it also slows down network speeds and takes up bandwidth as non stop packets are being sent through the network. It is safe to say that this is a serious attack, as if there are no ways to prevent this or stop it, then it could essentially run forever until the system is powered off. This is a huge security risk as this could prevent work from getting done, not only for the client being attacked, but also for other users on the network as well.

5. Ways to mitigate the attack

There are a few ways to ensure that a distributed denial-of-service attack will not negatively impact your network. The first line of defense should always come before the attack is initiated. By preemptively preparing for a potential cyber threat you can mitigate an attack completely or make the attack easier to counter if it does ever occur. A common counter measure that a system administrator can exercise in order to prepare are putting rate limits on the networks router in order to prevent the web server from being overwhelmed.This means the number of requests a server can accept within a certain timeframe has been limited. While this is a useful element of DDoS mitigation, it won't work when dealing with larger, more complex attacks.

If this method is not practical for the system administrator or if the attacks the network is suffering from is a more complex form of a DDOS attack, consider configuring your firewall or IDS (Intrusion Detection System) to filter DDoS traffic, if the functionality is available, or consider upgrading to a system that does. DDoS traffic filtering devices prevent SYN, TCP Flooding and other types of DDoS attacks. Such devices typically analyze TCP flow control, conduct packet filtering and utilize blacklists and whitelists to ensure any unwanted potentially malicious network traffic does not even make it to the server and some IDS systems have features that will notify the administrator of such attempts.