Identifying a DoS Attack

Dr Rob Hegarty

Overview

Incident response is a key part of computer security. To maintain the CIA (Confidentiality, Availability and Integrity) of an asset you must be able to respond accordingly to threats. Denial of Service Attacks are class of attack that aim to reduce or remove the availability of an asset. DoS attacks require very little skill, hacktivist groups have capitalised on this and offer tools such as Low Orbit Ion Cannon for members to use in their campaigns.

Distributed Denial of Service attacks (DDoS) are coordinated attacks using hundreds of thousands of machines. The machines involved are often part of a botnet. Botnets are zombie computers which have been infected by malware. Organised crime gangs run botnets and charge customers by the hour for their use.

In this lab session you are required to carry out a DoS attack, to develop an understanding of how these attacks function. This means that you will also be launching a DoS attack on your virtual network. Under no circumstances should you attack computer systems outside of your virtual network. The University and lecturer bear no responsibility for you actions and are duty bound to report infringements of the computer misuse act.

Task 1 – Computer Misuse Act

Read the computer misuse act from the link below and take a few moments to consider the implications:

http://www.legislation.gov.uk/ukpga/1990/18/contents

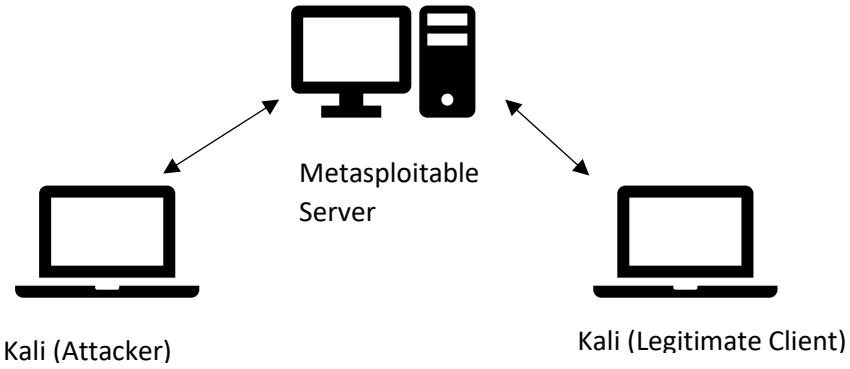
Note, launching a DoS attack will not make you “hot property” in the InfoSec world and get you hired by the men in black suites. If caught however you will have a criminal record which will have a serious impact on your career.

Task 2 – Installing a Kali Virtual Machine

Kali Linux is a penetration testing tool used widely in the security industry. Kali is a very powerful tool that should be used with care.

Kali is a LiveCD based operating system designed to be run entirely from a CD/DVD/USB drive, the core parts of the of and recently used applications are loaded into memory, and no data is written to the hard drive. LiveCD’s are useful for data recover, digital forensics, and activists who wish to leave behind little evidence of their computing activities.

Refer to the Week 2 lab session for detailed instructions on how to configure a VM. For this session you will deploy your existing Kali and Metasploitable virtual machines, **and an additional Kali virtual machine, to create the network shown in the figure below**. All machines should be on the NAT network you created in week 2. If you are using your own laptop use a host only network instead.



Check the IP address of each virtual machine ensure all virtual machine are on the same network and subnet. Make a note of the IP addresses of each machine.

Task 3 – Understanding DoS Attacks

To mitigate a DoS attack we must first understand how they work. So before launching a DoS attack in your virtual environment we will look briefly at a SYN Flood attack (also called a SYN-Connect attack), this is one of the most common types of DoS attack.

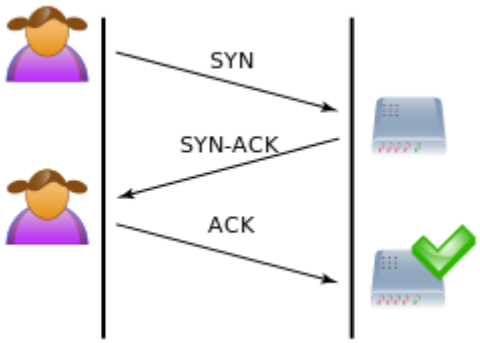
Before we can understand how a DoS attack works, some quick background is required on TCP/UDP. Both TCP and UDP run over IP and are part of the TCP/IP suite of protocols. TCP and UDP are transport protocols that reside at layer 4 of the OSI model. IP is a network protocol that resides at layer 3 of the OSI model.

OSI Model				
Layer		Protocol data unit (PDU)	Function[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access	DotNetFtpLibrary,[4] SMTP web API,[5] SSH.NET,[6] SnmpSharpNet,[7] HTML Class,[8] HTTP API server[9]
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	CSS, GIF, HTML, XML, JSON, S/MIME,
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, SCP, NFS, PAP, TLS, FTP,[10] HTTP,[11] HTTPS, SMTP,[12] SSH,[13] Telnet[14]
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	NBF, TCP, UDP
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	AppleTalk, ICMP, IPsec, IPv4, IPv6
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	IEEE 802.2, L2TP, LLDP, MAC, PPP, ATM, MPLS
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DOCSIS, DSL, Ethernet physical layer, ISDN, RS-232

More details can be found on the OSI Wikipedia page - http://tinyurl.com/cgkkokg

UDP is a best effort connectionless protocol, packets are transmitted but never acknowledged so transmission is not guaranteed. TCP on the other hand is a connected protocol, packet receipt is acknowledged, and delivery guaranteed.

TCP SYN Flood attacks or SYN-FLOODS subvert the TCP three-way handshake by initiating but never completing the handshake. The diagrams below illustrate how a normal three-way handshake is carried out and how a SYN-FLOOD works.

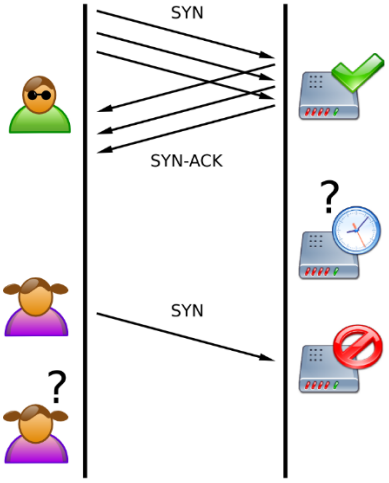


Standard three-way handshake

During the initiation of a TCP connection the client and server exchange SYN-ACK and ACK packets. Once these packets have been exchanged communication can begin.

When a SYN-FLOOD DoS attack is launched the attacker send many thousands of SYN requests to the server but never acknowledges the received SYN-ACK requests with an ACK response. This creates

half-open connections as the server is waiting for ACK responses to complete the initialization of the connections. For each ACK response the server is waiting for, it allocates some resources. If enough half-open connections are made, the server can no longer complete legitimate connections. This leads to legitimate user's being unable to access the server, which is the definition of a DoS attack.

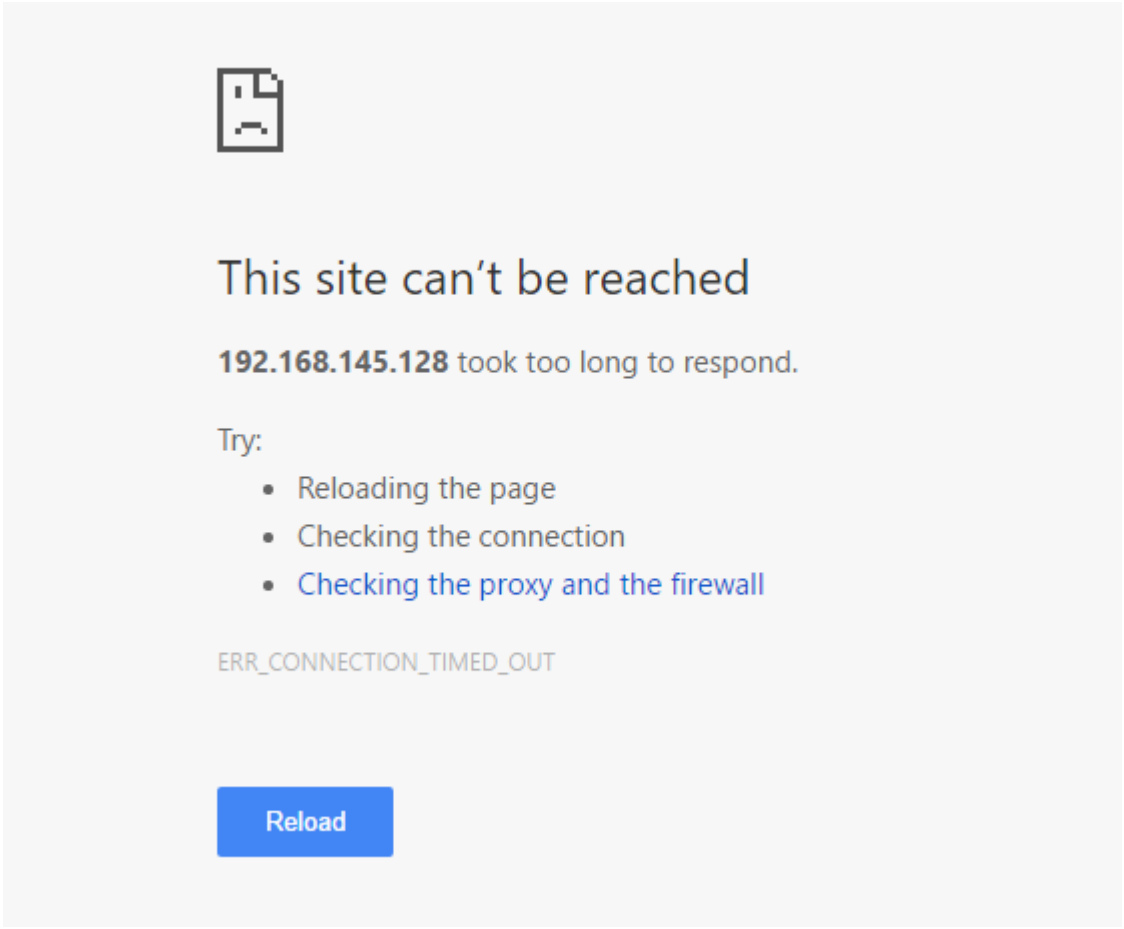


Launching a DoS Attack

To mitigate against a DoS, attack we must first launch an attack to demonstrate the effectiveness of our mitigation strategy.

To carry out and observe a DoS attack, a virtual webserver will be deployed and accessed via a web browser on a Kali virtual machine serving as a legitimate user. A second Kali virtual machines will be used to carry out a DoS attack, making the webserver inaccessible to the first legitimate Kali virtual machine.

1. Ensure you have introduced an execution cap, and limited the memory of the Metasploitable virtual machine to 512MB
2. Start your Metasploitable and **two Kali virtual machines**.
3. As you will be using two Kali virtual machines. Change the wallpaper on one of the machines so that you can differentiate between the machine acting as a legitimate machine, and the attack machine.
4. Find the IP address of the Metasploitable webserver by typing ifconfig on the Metasploitable virtual machine.
5. Start a web browser in private browsing mode on the legitimate Kali machine and visit the IP address of the Metasploitable virtual machine. You should see a rudimentary webpage.
6. Read the documentation on the Linux `nping` command:
    a. https://nmap.org/book/nping-man.html
7. Carry out Internet research on how to use `nping` to carry out a DoS attack using the attack Kali virtual machine against Metasploitable.
8. Carry out a TCP CONNECT DoS attack against the webserver from the Kali Linux VM. Document your attack and describe how it works.
9. To demonstrate the success of the DoS attack, attempt to access the webserver from a web browser on your host machine, if the attack is successful you will see a page like the one below:



Note you will need to make sure you refresh the webpage by holding down shift and hitting the refresh icon or pressing shift + F5 to ensure the web browser attempts to make a connection to the web server rather than displaying a cached version of the web page. Depending on the network configuration of your host machine it may be difficult to carry out a DoS, however you should try a few times, and observe the increase in time required to load the web page during a DoS.

Task 4 – Identifying a Denial of Service Attack

To identify a denial of service attack, you are going to observer the network connections on the Metasploitable machine using netstat.

- Review the documentation for `netstat` using the man pages.
- Observe a normal connection from the legitimate Kali machine browsing the web server, using netstat on the Metasploitable virtual machine.
- Carry out a TCP-Connect DoS attack on the Metasploitable virtual machine using the attack virtual machine. Observe the connections on Metasploitable virtual machine.
- Document the differences between legitimate and illegitimate connections, take note to the local address, foreign address, and state of each connection. Explain how the DoS works in your own words.

Extended Task

Despite the warning issued about Kali, it is an extremely useful and powerful tool. Take some time and explore the applications installed in Kali. There are plenty of online tutorials on Kali, many free of charge to access. Take the time to read some tutorials, please bear in mind some tutorial may be malicious in nature, recap on the computer misuse act before undertaking any of the tutorials.