ACM-CyberSecurity Summer Mentorship
Assignment-2

Mafiaboy(Feb 7,2000)

This attack was launched was by **Michael Calce** .He launched a series of denial-of-service attacks in February 2000 against large commercial websites including Amazon.com,CNN.com,eBAY and Yahoo.The hack cost 1.7billion dollars.

He had broken into 50 networks and had installed software called Sinkhole.He directed sinkhole to flood the targets with attack traffic.

Methods that could have been adopted to prevent this attack:

1. Configuring the network:As he had broken into 50 networks,configuring the network could have prevented it.Dropping junk packets,blocking requests from unnecessary ports are few things that could have been adopted.
2. Monitoring the network:It is very necessary to monitor the network to detect early traffic spiks.
3. As he had installed sinkhole software,by insatalling an antivirus to detect and delete that software is the easiest way to prevent it.

Case study:

- She has adjusted her firewall so that no incoming ICMP packets are allowed.It is better to apply filters in fire wall instead of blocking all the ICMP packets.

  It is true that ICMP does have some security issues associated with it and that lot of ICMP should be blocked,but there is no reason to block all ICMP traffic because ICMP has many important features which are useful for troubleshooting,while some are essential for network to function correctly.

- She has changed the web server so that it uses SYN cookies. The cryptographic hashing used in SYN cookies is fairly resource intensive,therefore another cookie method that is easier to implement than SYN cookie i.e RST cookie can be used.

- Following precautions can also be taken:
  1. As the network is divided into multiple segments separated by routers, configuring Internal routers to disallow any traffic that does not originate within the network.
  2. Disabling directed IP broadcasts on all routers.
  3. Filters on routers to check if external packets have external IP address and internal packs have internal IP address
  4. Always use virus-scanning software and keep it updated.

1.A firewall is a stateful device that is designated and configured to block undesired ports but ports 80,53,25 and 443 are always open because they are the entry point for desired service delivery traffic.The DDOS attacks occur on these open ports and therefore we can configure filters to check the packets going and out in these ports.

Another step that can be taken to defend against DDOS attack is by extending the bandwidth of the firewalls.The volumetric flood attack exploit the stateful nature of the firewall by filling up the state tables with volumes of unwanted traffic so that it has little time to pass legitimate traffic i.e 1-5 Gbps bandwidth is provided from Internet Service Provider but the average size of DDOS attack is 6.63Gbps. Though attackers may fill up extended bandwidth,it can be seen a mitigation step rather than defending.

Firewall provide perimeter access control by monitoring and tracking permitted network traffic flows.Firewalls can be helpful in detecting an incoming DDOS attack,but it can’t do much to defend against the attack.

2.Trojan is a piece of malware that pretends to be something bengin,such as media player,an emailed file etc seeing which users are deceived into opening file,which in most cases installs the malware.

Protecting against Trojan horse attacks reduce DoS attacks because:

- Many DOS attacks are conducted by using a Trojan horse to get an unsuspecting machine to execute the DOS.
- They install botnet software which makes the computer "infected" and links it with other infected computers,by which it can be secretly controlled by cybercrimanls without owner's knowledge.(Botnets are used for launching DDOS attacks).

3.The following are the ways to protect against SYN flood attack:

- Micro blocks
- SYN cookies
- RST cookies
- Stack tweaking