Joshua Main-Smith
October 18, 2020

DOS Attack Assignment

1. **(5 points) In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a10-Mbps link?**

   To generalize:
   ICMP packet size = P
   Packets per second = X
   Link Capacity = L
   P * X = L

   0.5 Mbps Link:
   P = 500 B
   X = ?
   L = 0.5 Mbps = 0.0625 MBps = 62500 Bps
   500 B * X = 62500 Bps => X = 62500 Bps / 500 B = 125 pps

   2 Mbps Link:
   P = 500 B
   X = ?
   L = 2 Mbps = 0.25 MBps = 250000 Bps
   500 B * X = 250000 => X = 250000 Bps / 500 B = 500 pps

   10 Mbps Link:
   P = 500 B
   X = ?
   L = 10 Mbps = 1.25 MBps = 1250000 Bps
   500 B * X = 1250000 Bps => X = 1250000 Bps / 500 B = 2500 pps

   *Graph of relationship shown at the bottom. With the relationship being linear, one can easily see how many pps are needed to flood an organization given its link capacity, given packet size in 500 Bytes.
   In other words, 250 pps/Mbps is what’s needed for flooding (250 * 10 Mbps = 2500 pps, e.g.).

2. **(10 points) Consider a distributed variant of the attack we explore in Problem 1. Assume the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 128 Kbps. What is the maximum number of 500-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a 10-Mbps link? Given reports of botnets composed of many thousands of zombie systems, what can you conclude about their controller's ability to launch DDoS attacks on multiple such organizations simultaneously? Or on a major organization with multiple, much larger network links than we have considered in these problems?**

   To generalize:
   ICMP packet size = P
   Packets per second = X
   Uplink Capacity = L
   P * X = L

   Packets per second for each PC:
   P = 500 B
   X = ?
   L = 128 Kbps = 16 KBps = 16000 Bps
   500 B * X = 16000 Bps   =>   X = 16000 Bps / 500 B = 32 pps/per PC

   Number of PCs needed for
   0.5 Mbps Link:
   From above, 125 pps needed to flood organization.
   125 pps / (32 pps / per PC) = 3.9 PCs = 4 PCs needed to flood organization (rounding up).

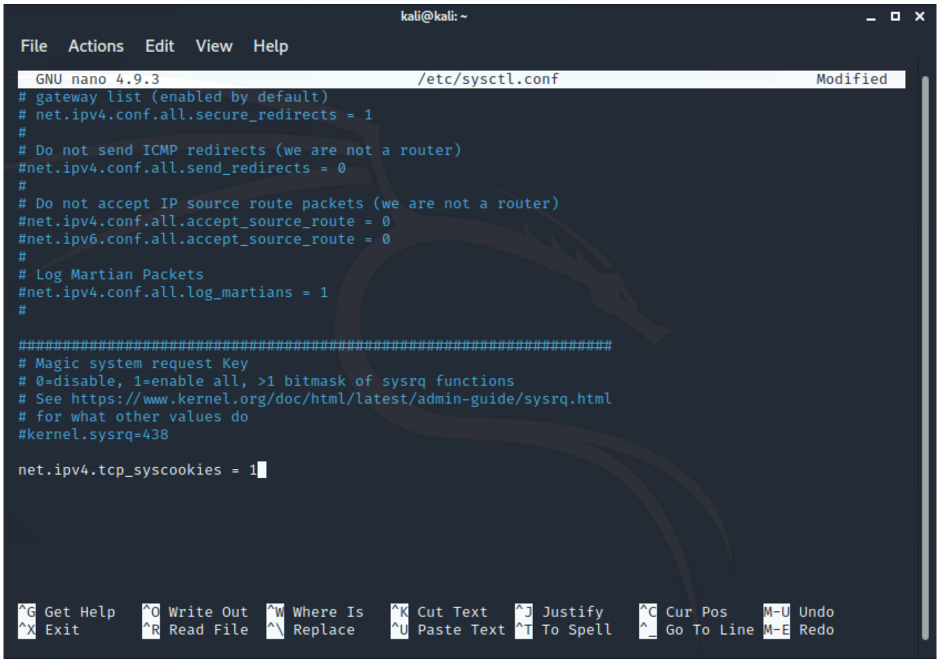
   2 Mbps Link:
   From above, 500 pps needed to flood organization.
   500 pps / (32 pps / per PC) = 15.625 PCs = 16 PCs needed to flood organization (rounding up).

   10 Mbps Link:
   From above, 2500 pps needed to flood organization.
   2500 pps / (32 pps / per PC) = 78.125 PCs = 79 PCs needed to flood organization (rounding up).

   I was surprised to see how little PCs are actually needed in performing DOS attacks. It's no surprise that individuals/organizations that have access to hundreds or thousands of PCs can easily cripple a target. As technology improves, smaller businesses may suffer the most. Consumers will continue to have access to more powerful machinery. With the average uptick speed increasing per user, an attacker's botnet becomes more powerful. Smaller organizations that are unable to support the cost of withstanding large traffic are highly susceptible to these sorts of attacks.

3. **(10 points) Research whether SYN cookies, or other similar mechanism, are supported on an operating system you have access to (e.g., BSD, Linux, MacOSX, Solaris, Windows). If so, determine whether they are enabled by default and, if not, how to enable them.**

   SYN cookies are available on my Kali distribution. To enable SYN cookies, we can go to the config file using the command **nano /etc/sysctl.conf**, then append **net.ipv4.tcp_syncookies = 1** to the file, as shown in the screenshot below (Reference).



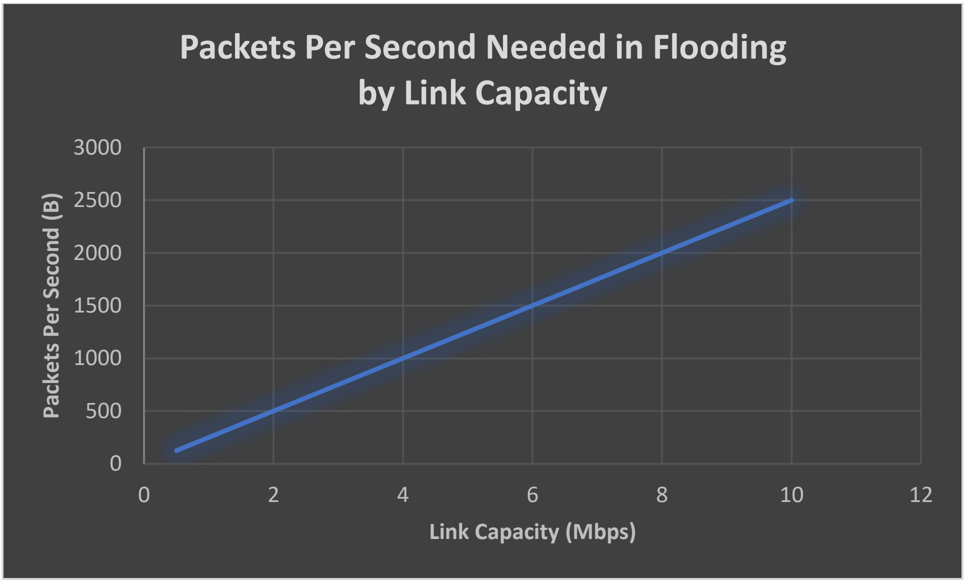
```
  GNU nano 4.9.3                         /etc/sysctl.conf                               Modified
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#

###################################################################
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438

net.ipv4.tcp_syscookies = 1
```

4. **(10 points) Research how to implement antispoofing and directed broadcast filters on some type of router (perhaps the type your organization uses).**

   In a CISCO router, antispoofing can be enabled by going to the firewall settings. Under access control list (ACL), inbound ACL will allow anti-spoofing filters to be put into place. Click **Apply Firewall**, and a window will appear showing the changes. Click **Ok** to accept the changes.

   Directed broadcast can be disabled by issuing the command **no ip directed-broadcast** into the command line interface to the router. This can be undone by running the Security Audit Wizard, then go to Under Security Configuration and then put a check mark next to directed broadcast (or whichever security audit wished to be undone).

   Reference


Packets Per Second Needed in Flooding by Link Capacity
Packets Per Second (B)
3000
2500
2000
1500
1000
500
0
0
2
4
6
8
10
12
Link Capacity (Mbps)