**Companion Notes**

HPing is a packet sniffer, also known as a packet analyzer, protocol analyzer or network analyzer. A packet sniffer is a hardware or software used to monitor network traffic. Sniffer examines the streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet. These packets are intended for and addressed to specific machines but using a packet sniffer in "promiscuous mode" allows IT professionals, end users or malicious intruders to examine any type of packet, regardless of destination. Sniffers could be configured in two ways. The first is "unfiltered," meaning this will capture all packets possible and write them to a local hard drive for later examination. Next is the "filtered" mode, meaning analyzers will only capture packets that contain specific data elements.



Packet sniffers can be used on both wired and wireless networks. Their efficiency depends on how much they are able to "see" as a result of network security protocols. On a wired network, sniffers might need access to the packets of each connected machine or could also be restricted by the location of network switches. On a wireless network, most sniffers will solely scan one channel at a time, however the employment of multiple wireless interfaces will expand this capability.

**Prevalence and Risk Factors**

Using a sniffer, we can capture any information-: for example, the websites that a user visits, what is viewed on the site, the contents and destination of any email along with details about any downloaded files. Protocol analyzers are usually utilized by firms to stay track of network use by staff and are part of the many respectable antivirus code packages. Outward-facing sniffers scan incoming network traffic for specific parts of malicious code, serving to forestall bug infections and limit the unfold of malware.

These analyzers also can be used for malicious functions. If a user is convinced to transfer malware-laden email attachments or infected files from an internet site, it's potential for AN unauthorized packet mortal to be put in on a company network. Once in place, the packet sniffer can record data transmitted and send it to a command and control (C&C) server for further analysis. It's then possible for hackers to attempt packet injection or man-in-the-middle attacks, along with compromising any data that was not encrypted before being sent.

While Hping was mainly used as a security tool in the past, it can be used in many ways by people that don’t care about security to test networks and hosts. A subset of the stuff you can do using Hping:

* Firewall testing
* Advanced port scanning
* Network testing, using different protocols, TOS, fragmentation
* Manual path MTU discovery
* Advanced traceroute, under all the supported protocols
* Remote OS fingerprinting
* Remote uptime guessing
* TCP/IP stacks auditing
* Hping can also be useful to students that are learning TCP/IP.

Attacks using hping3

DOS attack

An attack meant to shut down a machine or network, making it inaccessible to its intended users by flooding it with traffic.

SYN Flooding

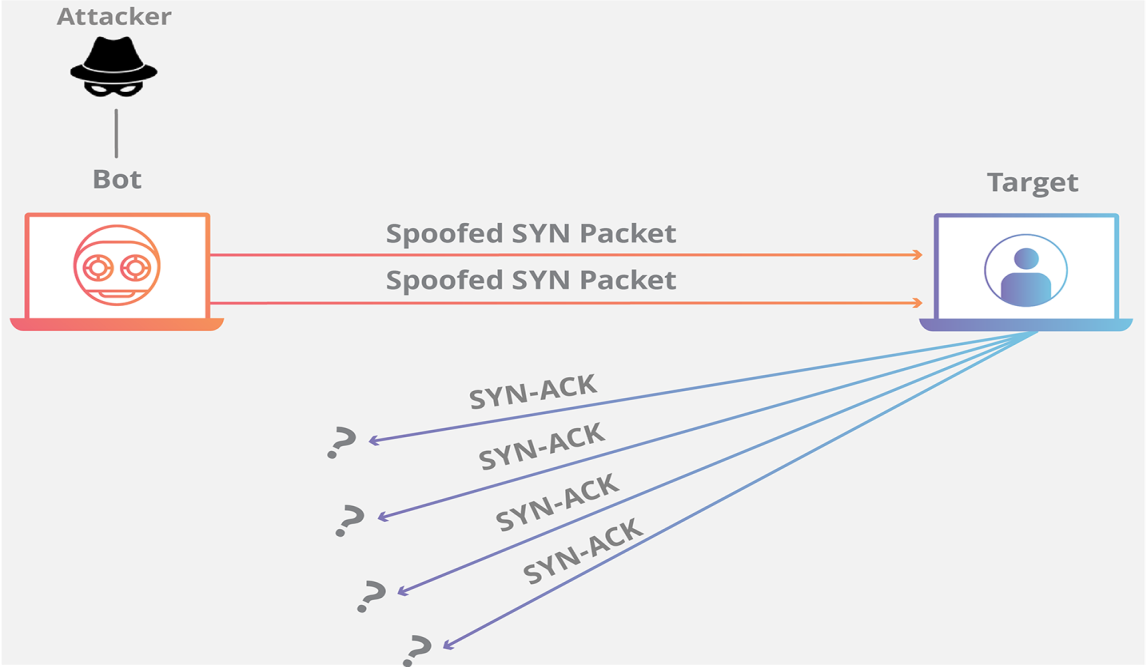
SYN flood attacks work by exploiting the 3 way handshake process of a TCP connection. A SYN flood is a form of [DOS attack](https://en.wikipedia.org/wiki/Denial-of-service_attack) in which an attacker [SYN](https://en.wikipedia.org/wiki/SYN_(TCP)) requests successively to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. This is how the TCP 3-way-handshake process works:-

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

A SYN flood attack works by not responding to the server with the expected ACK code. The attacker can either simply not send the expected ACK, or by [spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing) the source [IP address](https://en.wikipedia.org/wiki/IP_address) in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN.

Countermeasures

1. Filtering
2. SYN Cache
3. [SYN cookies](https://en.wikipedia.org/wiki/SYN_cookies)
4. Firewalls and Proxies

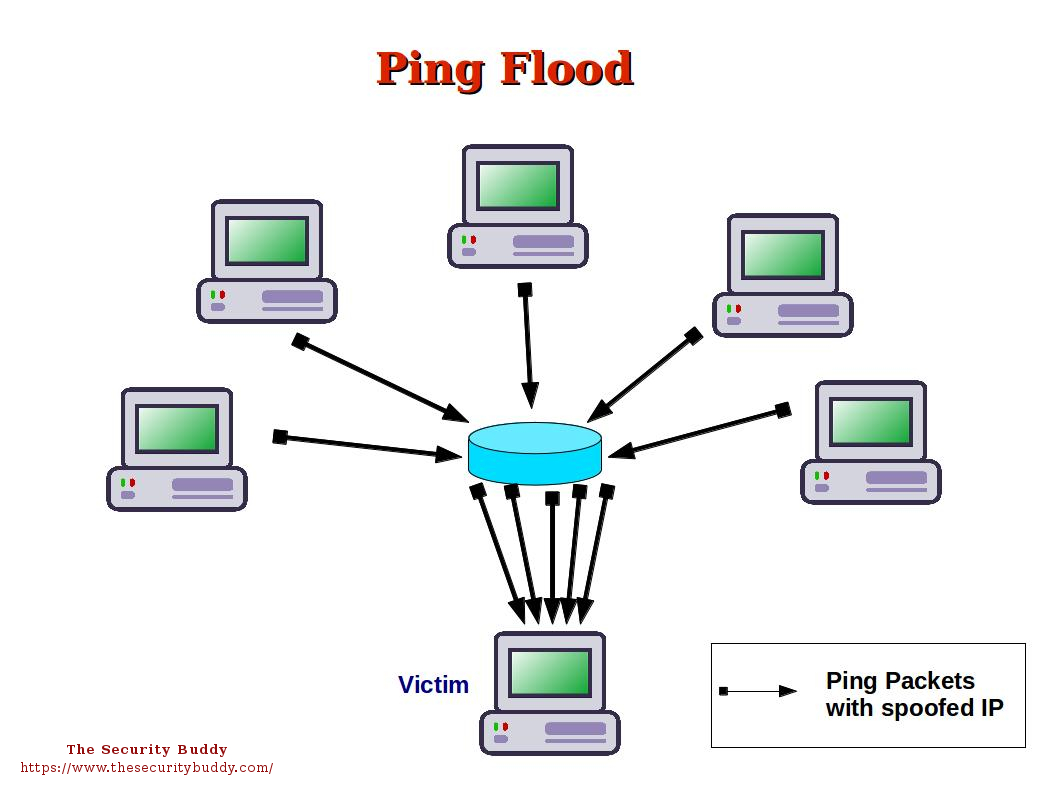


ICMP Flooding

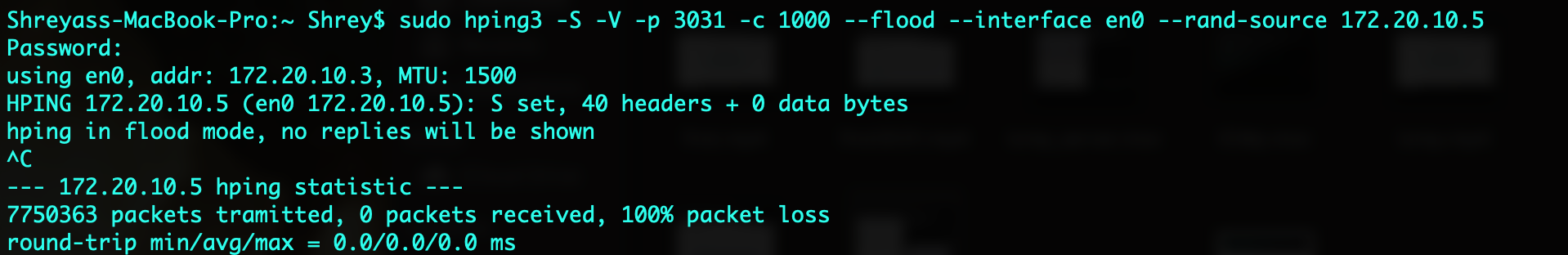
A ping flood could be a straightforward denial-of-service attack wherever the attacker overwhelms the victim with ICMP "echo request" (ping) packets. this is often best by exploiting the flood possibility of ping that sends ICMP packets as fast as possible while not expecting replies.  
This attack is a DDOS attack within which large numbers of internet control Message Protocol (ICMP) packets with the victim's spoofed source ip are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, reply to this by sending a reply to the source ip address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer are going to be flooded with traffic. this can slow down the victim's computer to the purpose where it becomes impossible to carry on.

Counter measures:

1. Configure individual hosts and routers to not respond to ICMP requests or broadcasts
2. Configure routers to not forward packets directed to broadcast addresses.

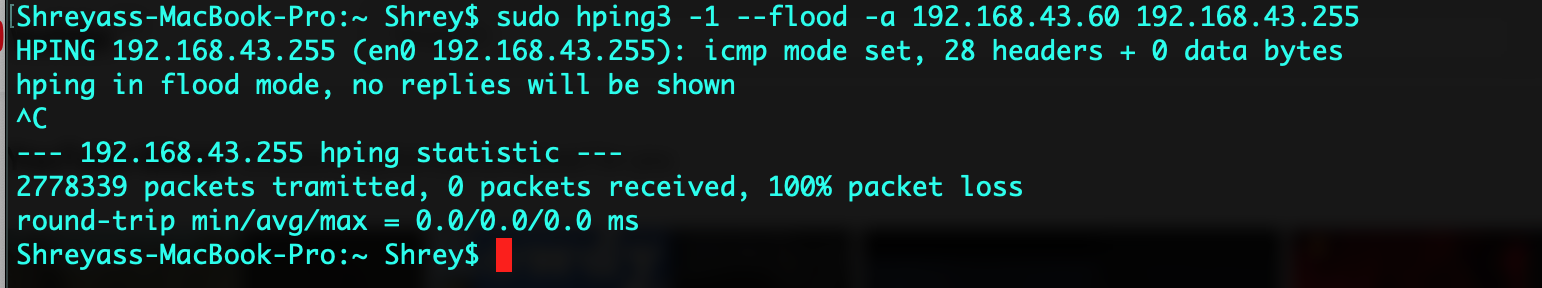


**Syn-Flood Attack**



The command above describes the Syn-Flood attack. The -S flag is used to specify Syn packets. The -V flag is for Verbose. The -p flag describes the port to attack on the victim’s IP address. The -c flag specifies the number of packets to be sent (count). There is a flood flag as well and the interface specifies the attacker’s interface, in this case it is WiFi. The –rand-source followed by the victim’s IP address specifies that the SYN packets need to be sent to the victim assuming random IP addresses in the network. Hence the SYN-ACK replies will be sent to other IP addresses. This causes the application running on the particular IP address and port number to crash.

**ICMP Flood Attack:**



*hping3 -1 - -flood -a <VICTIM\_IP> <VICTIM\_NETWORK\_RANGE>*

flag descriptions:

* -1: Specifics ICMP flood mode in hping3 command-line
* -a: Specifics the VICTIM\_IP address
* --flood: Specifies flood attack

The above command specifies the ICMP flood attack on the <VICTIM\_IP> and the ping requests are broadcast to the <VICTIM\_NETWORK\_RANGE>

References:

<https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer>

<http://www.hping.org>

Videos on Youtube