Intro to Scapy

All Your Packets Are Belong To Us

Getting Scapy

See if your favorite Linux distribution has it.

apt-get install scapy || yum install scapy

http://www.secdev.org/projects/scapy/

Getting PCaps

http://www.netresec.com/?page=PcapFiles

https://github.com/markofu/pcaps

https://wiki.wireshark.org/SampleCaptures#Sample_Captures

Tutorials

http://packetlife.net/blog/2011/may/23/introduction-scapy/

http://www.secdev.org/projects/scapy/doc/usage.html

http://www.securitytube.net/tags/scapy

https://thepacketgeek.com/series/building-network-tools-with-scapy/

Using Scapy

Running the scapy command will give you an interactive shell for manipulating packets.

You can also import scapy into a Python script or into the interactive Python shell.

We'll be using scripts.

Creating Packets

Packets are created in layers.

Ethernet -> IP -> TCP|UDP -> Application

Use the / operator to join the various layers.

Look at create_packet.py

Process A Pcap: I

Packets are built from an Ethernet frame up through multiple layers.

An Ethernet frame has a payload, which is the IP packet.

An IP packet has a payload, which is either a TCP or UDP packet.

Look at process_pcap.py

Process A Pcap: II

Instead of working through each of these payloads, the data can be accessed directly.

Look at process_pcap2.py

Sniffing Packets

http://www.ccs.neu.edu/home/amislove/teaching/cs4700/fall09/handouts/project1-primer.pdf

http://itgeekchronicles.co.uk/2014/05/12/scapy-iterating-over-dns-responses/

Look at sniff_dns.py

Sending Packets

send - Send a layer 3 packet or packet set.
Do not wait for an answer.

sendp - Send a layer 2 packet or packet set.
Do not wait for an answer.

Look at send.py

Send and Receive Packets

Scapy operates at the user level not the kernel level. When you send packets with Scapy the kernel won't recognize the responses and will send a RST. You can get around that behavior by following the directions here:

https://isc.sans.edu/forums/diary/TCP+Fuzzing+with+Scapy/14080/

Send and Receive Packets

sr - Send a layer 3 packet and receive a list of answered and unanswered packets.

srp - Send a layer 2 packet and receive a list of answered and unanswered packets.

Look at send_recv.py

Send and Receive Packets

srp1 - Send a layer 2 packet or packet set and receive one answer.

sr1 - Send a layer 3 packet or packet set and receive one answer.

Look at handshake.py

Rewriting Packets

We can sniff packets and rewrite them on the fly.

Look at rewrite.py

Questions

stephen@averagesecurityguy.info

@averagesecguy

https://github.com/averagesecurityguy/scapy