VirginiaTech
Invent the Future

Networking Tools

ECE 4564 - Network Application Design

Dr. William O. Plymale

ece
BRADLEY DEPARTMENT
of ELECTRICAL & COMPUTER ENGINEERING

Topics

- Unix Network Commands
- Network Tools
- Python Network Code

Unix Network Commands

- ping
- netstat
- nmap
- netdata
- tcpdump

Linux Howto's

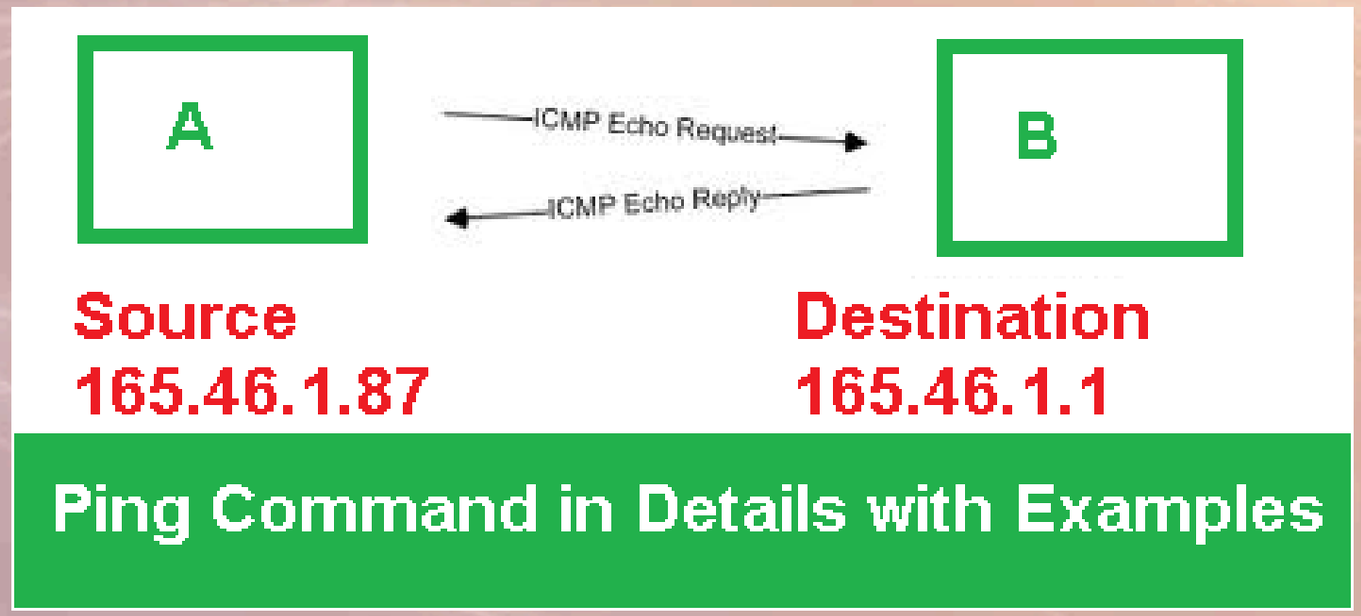
Tecmint

Linux Network Config and Troubleshooting

ping

Ping is a computer network administration utility used

- To test the reachability of a host on an Internet Protocol (IP) network
- To measure the round-trip time for messages sent from the originating host to a destination computer
- Name comes from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater



netstat

netstat (network statistics) is a command-line tool that

- displays network connections (both incoming and outgoing)
- routing tables
- network interfaces
- network protocol statistics

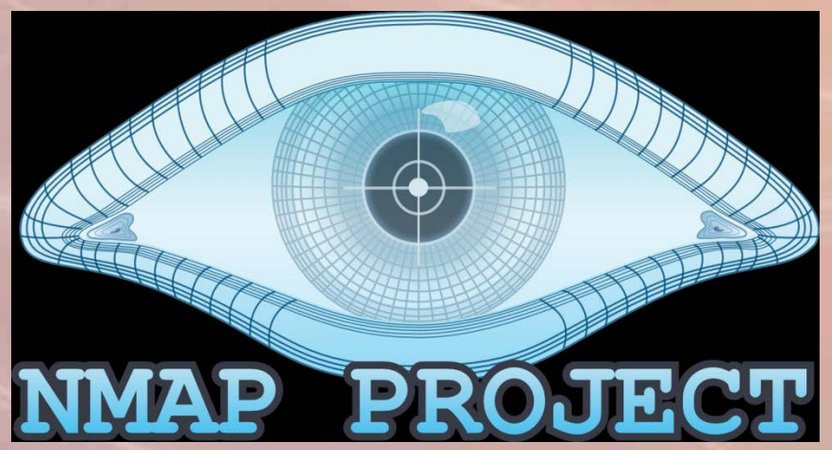
http://www.tecmint.com/20-netstat-commands-for-linux-network-management/

nmap

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

Useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics



http://nmap.org/

VirginiaTech
Invent the Future

netdata

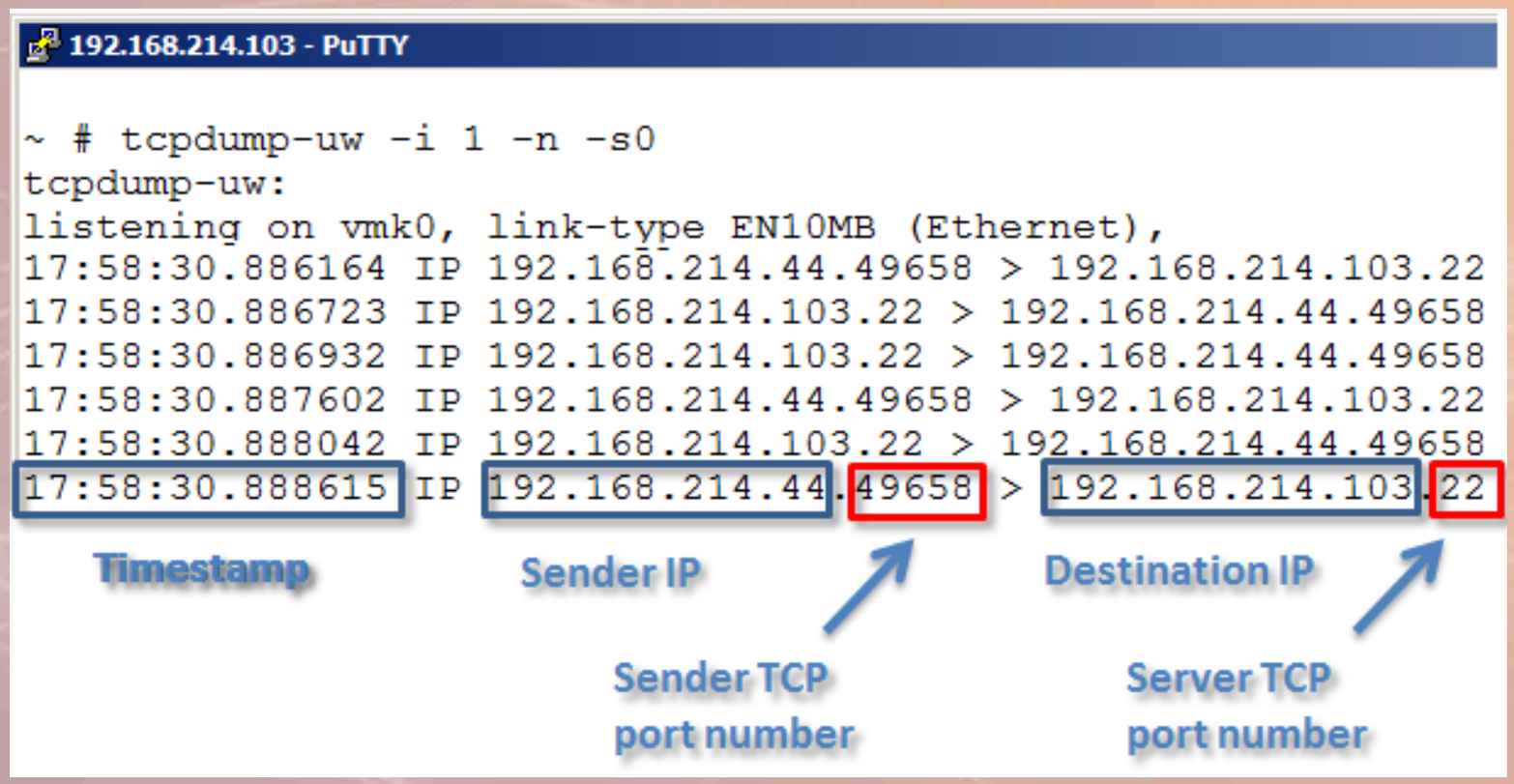
A Real-Time Performance Monitoring Tool for Linux Systems

http://www.tecmint.com/netdata-real-time-linux-performance-network-monitoring-tool/

ece
BRADLEY DEPARTMENT
of ELECTRICAL & COMPUTER ENGINEERING

tcpdump

- tcpdump is a common packet analyzer that runs under the command line.
- It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.



tcpdump

tcpdump

tcpdump -s 0 port ftp or ssh -i eth0 -w mycap.pcap

In above command

- -s 0 will set the capture byte to its maximum i.e. 65535, after this capture file will not truncate.
- -i eth0 is using to give Ethernet interface, which you to capture. Default is eth0, if you not use this option.
- port ftp or ssh is the filter, which will capture only ftp and ssh packets.
- -w mypcap.pcap will create a pcap file

pcap files are data files created using the program and they contain the packet data of a network.

Unix Network Tools

Wireshark

Top 20 Free Network Monitoring and Analysis Tools for Sys Admins

Wireshark

Wireshark is a free and open-source packet/protocol analyzer.

https://www.wireshark.org/

It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Wireshark is cross-platform, running on GNU/Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is a terminal-based (non-GUI) version called TShark.

Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark

Wireshark is software that "understands" the structure (encapsulation) of different networking protocols.

It can parse and display the fields, along with their meanings as specified by different networking protocols.

Wireshark uses *pcap* to capture packets, so it can only capture packets on the types of networks that *pcap* supports.

Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.

Wireshark

Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

Data display can be refined using a display filter.

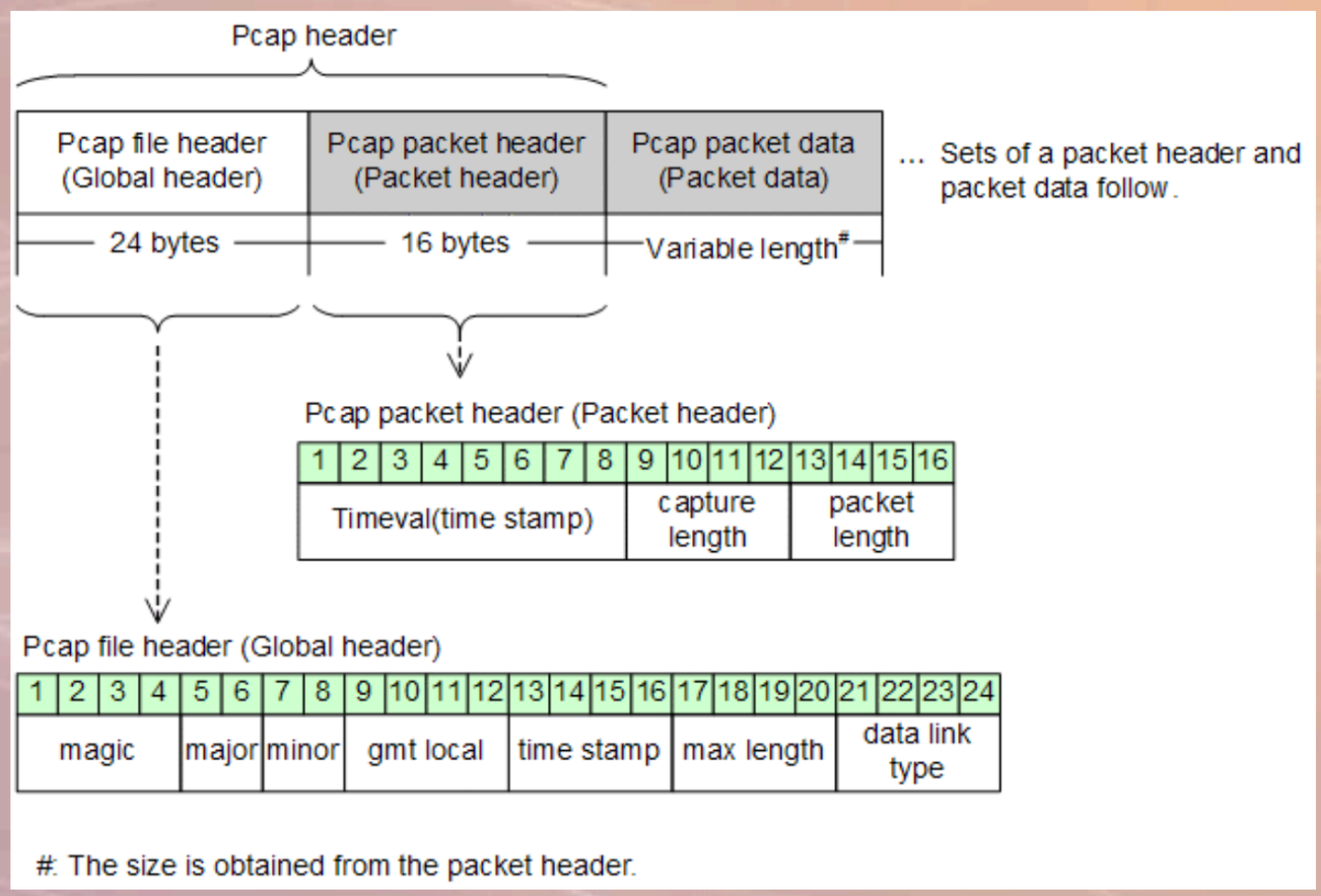
Plug-ins can be created for dissecting new protocols.

Wireshark is perhaps one of the best open source packet analyzers available today for UNIX and Windows.

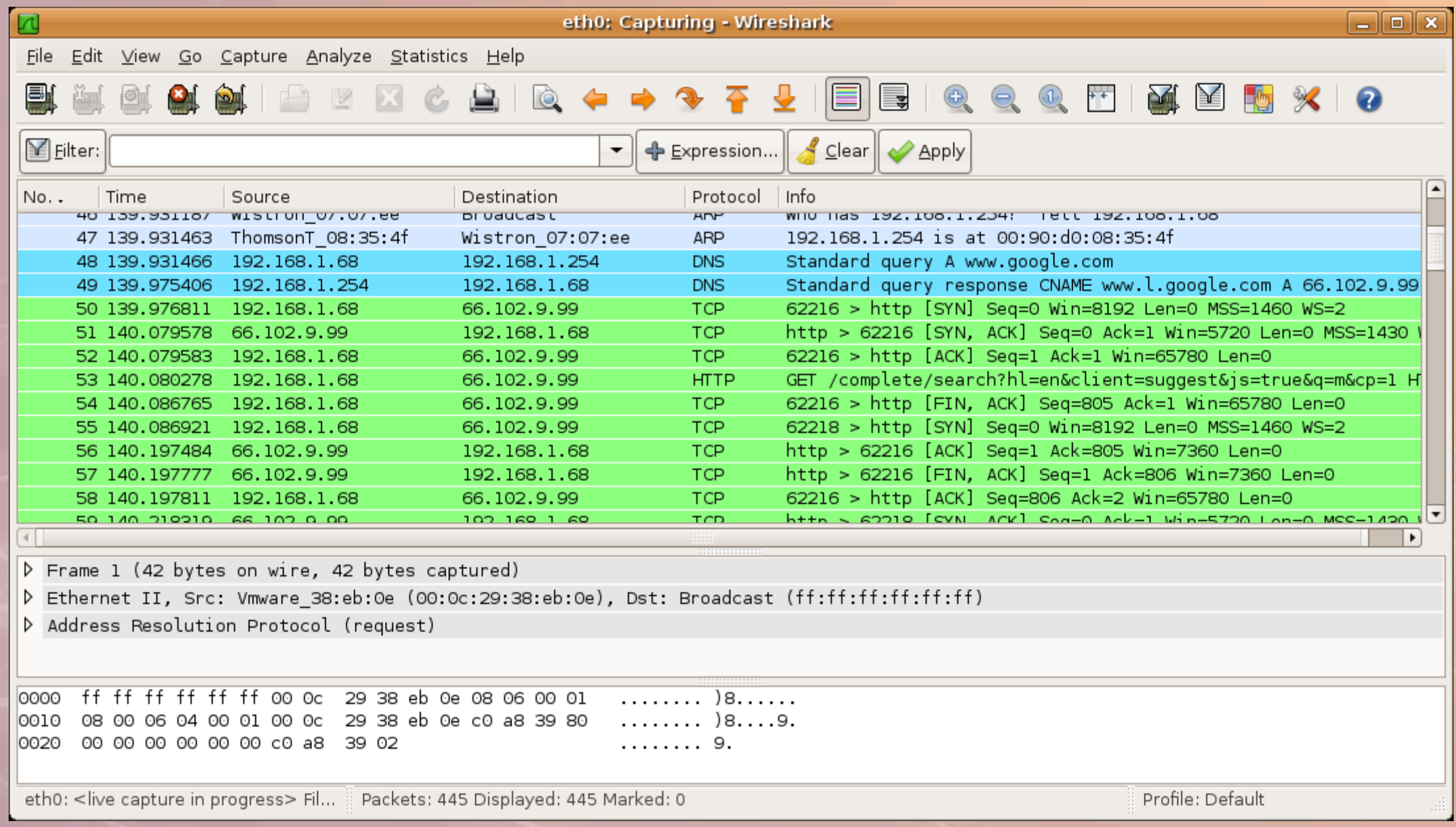
pcap

pcap (packet capture) consists of an application programming interface (API) for capturing network traffic

Unix-like systems implement pcap in the libpcap library
Windows uses a port of libpcap known as WinPcap.

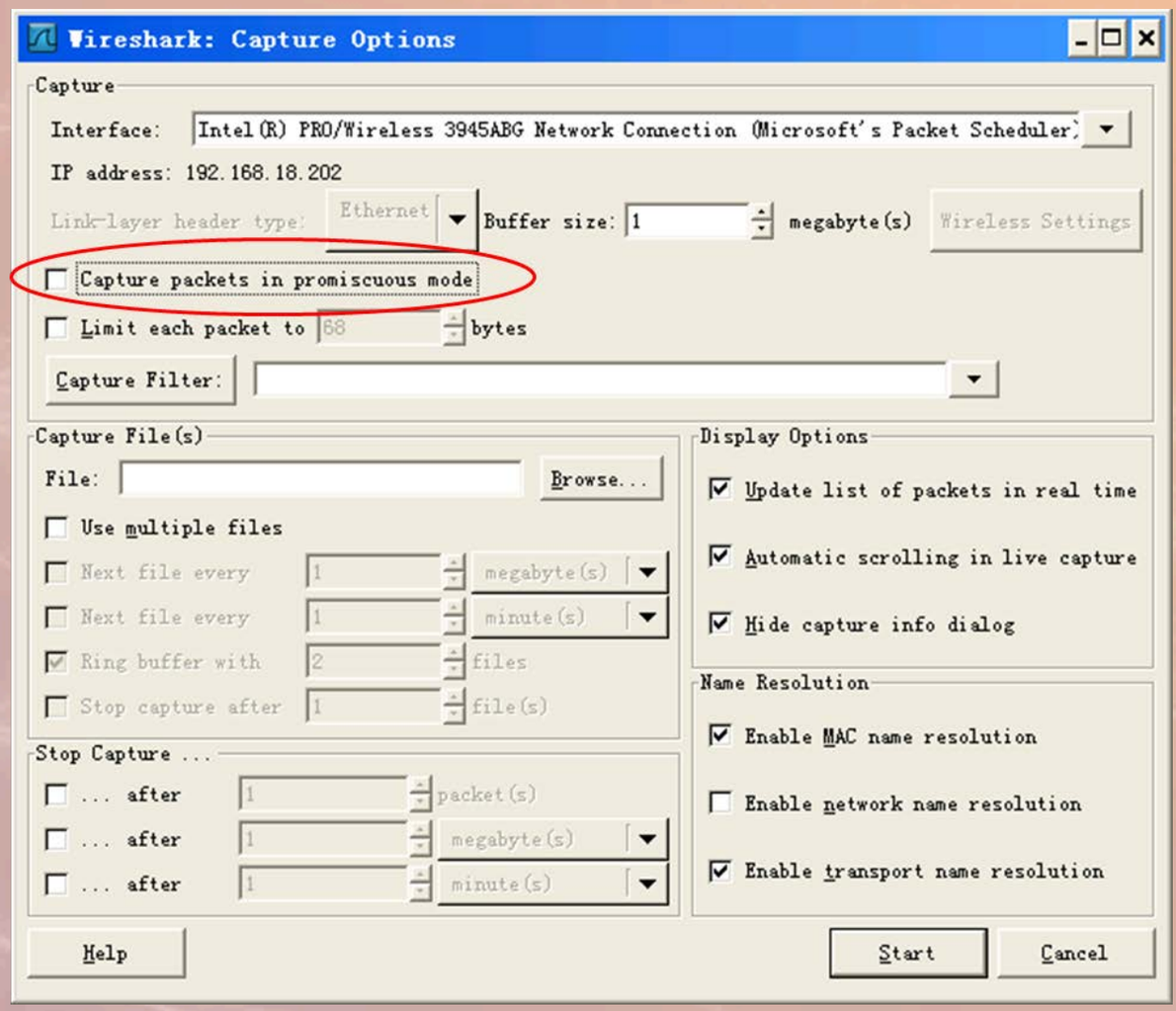


Wireshark

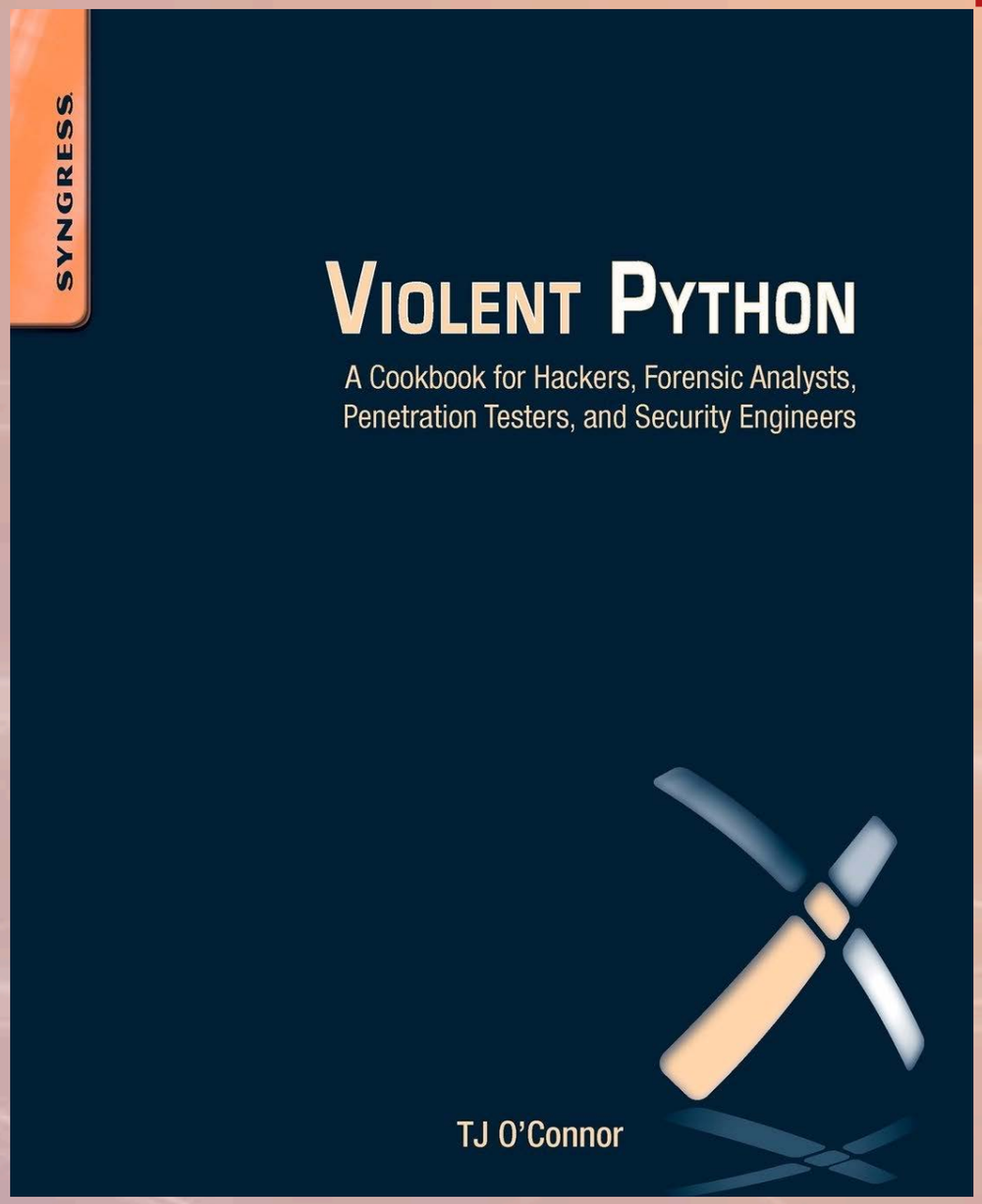

eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Configuration

This checkbox allows you to specify that Wireshark should put the interface in promiscuous mode when capturing. If you do not specify this, Wireshark will only capture the packets going to or from your computer (not all packets on your LAN segment).



Python Network Apps



https://github.com/shadow-box/Violent-Python-Examples

Scapy

Scapy is a powerful interactive packet manipulation program.

- able to forge or decode packets of a wide number of protocols
- send packets on the wire
- capture packets
- match requests and replies
- can handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery
- can also send invalid frames or inject your own 802.11 frames,

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

Scapy

"The Very Unofficial Dummies Guide to Scapy"

Adam Maxwell

Installation

1. Install Python 2.5+
2. Download and install Scapy

sudo apt-get install python-scapy

3. (Optional): Install additional software for special features.

apt-get install tcpdump graphviz imagemagick python-gnuplot python-crypto python-pyx

4. Run Scapy with root privileges.

https://theitgeekchronicles.files.wordpress.com/2012/05/scapyguide1.pdf

Scapy

Welcome to Scapy (2.2.0)

>>> send(IP(dst="127.0.0.1")/ICMP()/"HelloWorld")

Sent 1 packets.

>>>

send - this tells Scapy that you want to send a packet (just a single packet)

IP - the type of packet you want to create, in this case an IP packet

(dst=”127.0.0.1”) - the destination to send the packet to (in this case my router)

/ICMP() - you want to create an ICMP packet with the default values provided by Scapy

/”HelloWorld”) - the payload to include in the ICMP packet (you don’t have to provide this in order

for it to work.

VirginiaTech
Invent the Future

Scapy

Scapy Basics

Scapy

"Packet Wizardry Ruling the Network with Python"
Rob Klein

Scan an entire C-Class network for all hosts running that have port 80 listening.

```
p=IP(dst="hackaholic.org/24")/TCP(dport=80, flags="S")
sr(p)

results = _[0]

for pout, pin in results:
...    if pin.flags == 2:
...        print (pout.dst)
```

Scapy

Created a packet which was sent to the /24-subnet that hackaholic.org is connected to and set the TCP header to destination port 80 and the SYN flag.

The SYN flag is used to initiate a connection.

A reply of SA (SYN/ACK) means the port is listening, a RA (RESET/ACK) means it is closed, and finally no response means the host is down or filters packets.

After constructing the packet, Scapy emits the packets.

The results are then dissected in the for-loop and the destination IP addresses of hosts that replied SA are listed.

Closing