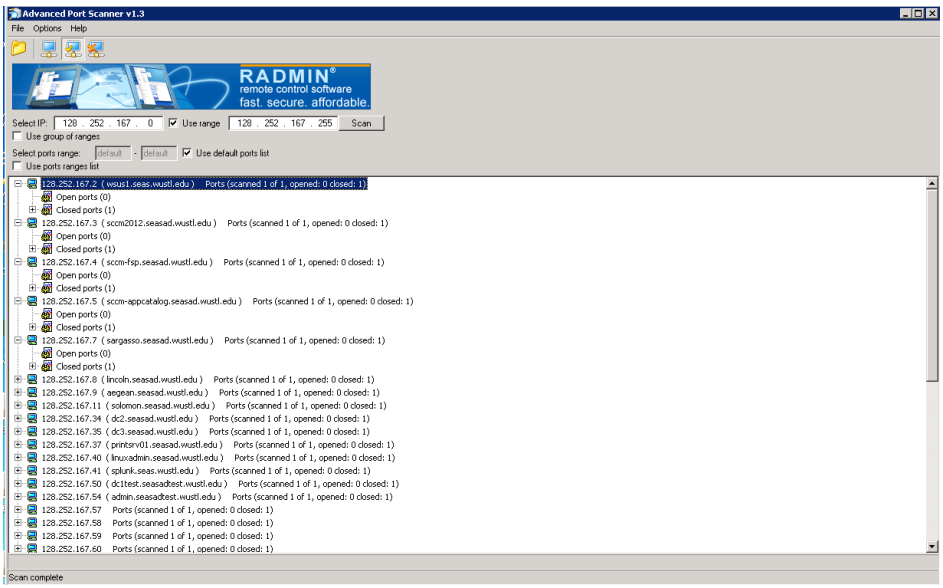
Network Security Lab 2

Network Security Lab 2

David Ayeke Jan 30. 2017

1. Scan of Advance Port Scanner



2. Use nmap to show the map of all host on your local net

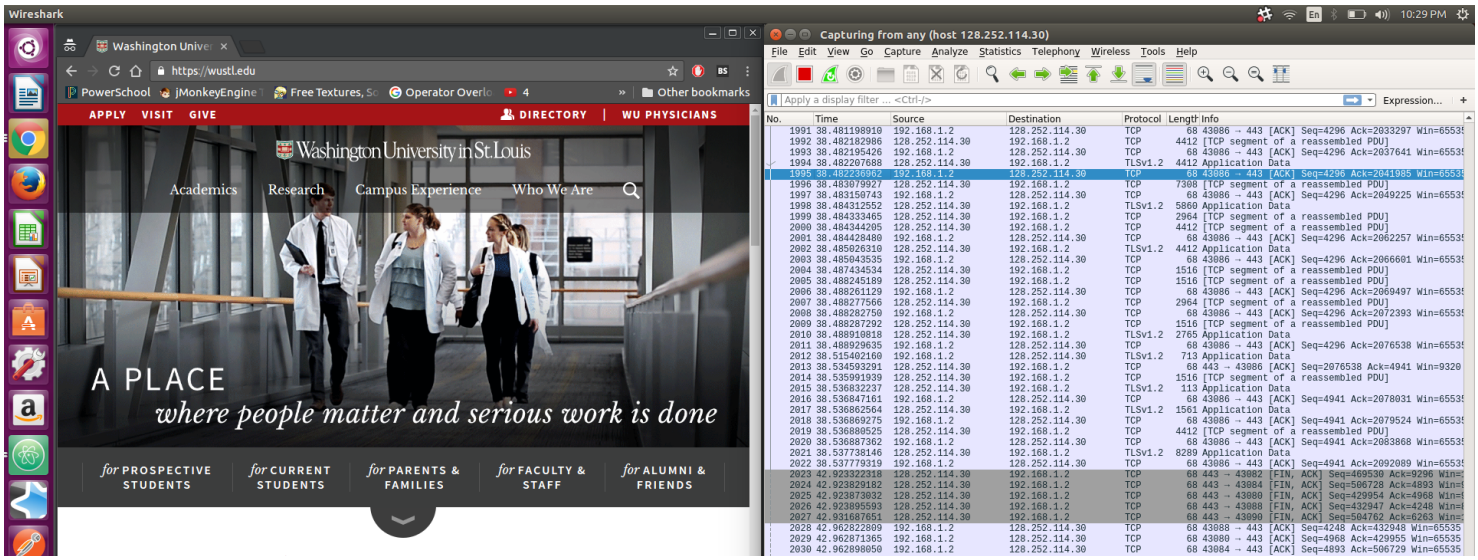
```
david@yogata:~/Downloads$ sudo nmap -sP 192.168.1.*

Starting Nmap 7.01 ( https://nmap.org ) at 2017-01-29 22:23 CST
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
```

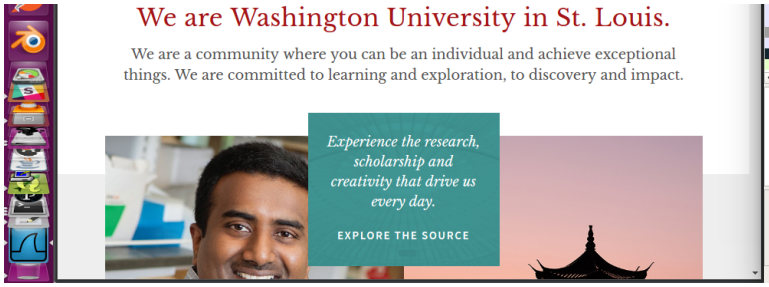
```
Host is up (0.0063s latency).
MAC Address: A0:63:91:AB:F1:2C (Netgear)
Nmap scan report for 192.168.1.3
Host is up (0.0063s latency).
MAC Address: 0C:FE:45:D7:75:35 (Sony)
Nmap scan report for 192.168.1.6
Host is up (0.017s latency).
MAC Address: C0:BD:D1:B2:B4:BB (Samsung Electro Mechanics)
Nmap scan report for 192.168.1.9
Host is up (0.027s latency).
MAC Address: B8:27:EB:96:42:18 (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.10
Host is up (0.027s latency).
MAC Address: B8:27:EB:41:47:32 (Raspberry Pi Foundation)
Nmap scan report for rpi0 (192.168.1.11)
Host is up (0.038s latency).
MAC Address: B8:27:EB:57:CD:0F (Raspberry Pi Foundation)
Nmap scan report for rpi3 (192.168.1.15)
Host is up (-0.067s latency).
MAC Address: B8:27:EB:A0:0B:BB (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.18
Host is up (-0.085s latency).
MAC Address: 90:B6:86:16:13:24 (Murata Manufacturing)

Nmap scan report for 192.168.1.110
Host is up (-0.085s latency).
MAC Address: 00:22:64:C9:31:B0 (Hewlett Packard)
Nmap scan report for 192.168.1.2
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 4.60 seconds
```

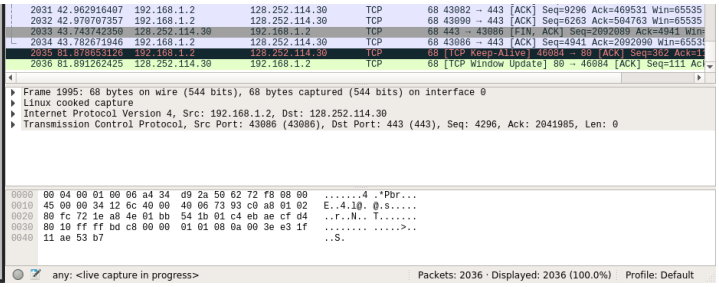
3. Capture all traffic from wireshark

First ping www.wustl.edu

```
david@yogata:~/Downloads$ ping www.wustl.edu
PING wordpress-prod.g.wustl.edu (128.252.114.30) 56(84) bytes of data.
64 bytes from wustl.edu (128.252.114.30): icmp_seq=1 ttl=242 time=15.0 ms
...
^C
--- wordpress-prod.g.wustl.edu ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17026ms
rtt min/avg/max/mdev = 13.157/14.561/23.761/2.427 ms
david@yogata:~/Downloads$
```




We are Washington University in St. Louis.
We are a community where you can be an individual and achieve exceptional things. We are committed to learning and exploration, to discovery and impact.
Experience the research, scholarship and creativity that drive us every day.
EXPLORE THE SOURCE


2031 42.962916407 192.168.1.2 128.252.114.30 TCP 68 43082 → 443 [ACK] Seq=9296 Ack=469531 Win=65535
2032 42.970707357 192.168.1.2 128.252.114.30 TCP 68 43090 → 443 [ACK] Seq=6263 Ack=504763 Win=65535
2033 43.743742350 128.252.114.30 192.168.1.2 TCP 68 443 → 43086 [FIN, ACK] Seq=2092089 Ack=4941 Win
2034 43.782671946 192.168.1.2 128.252.114.30 TCP 68 43086 → 443 [ACK] Seq=4941 Ack=2092090 Win=65535
2035 81.876053126 192.168.1.2 128.252.114.30 TCP 68 [TCP Keep-Alive] 46084 → 80 [ACK] Seq=362 Ack=1
2036 81.891262425 128.252.114.30 192.168.1.2 TCP 68 [TCP Window Update] 80 → 46084 [ACK] Seq=111 Ack
Frame 1995: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.252.114.30
Transmission Control Protocol, Src Port: 43086 (43086), Dst Port: 443 (443), Seq: 4296, Ack: 2041985, Len: 0
0000 00 04 00 01 00 06 a4 34 d9 2a 50 62 72 f8 08 00 ....4 .*Pbr...
0010 45 00 00 34 12 6c 40 00 40 06 73 93 c0 a8 01 02 E..4.l@. @.s.....
0020 80 fc 72 1e a8 4e 01 bb 54 1b 01 c4 eb ae cf d4 ..r..N.. T.......
0030 80 10 ff ff bd c8 00 00 01 01 08 0a 00 3e e3 1f ....>..
0040 11 ae 53 b7 ..S.
any: <live capture in progress>
Packets: 2036 · Displayed: 2036 (100.0%)
Profile: Default