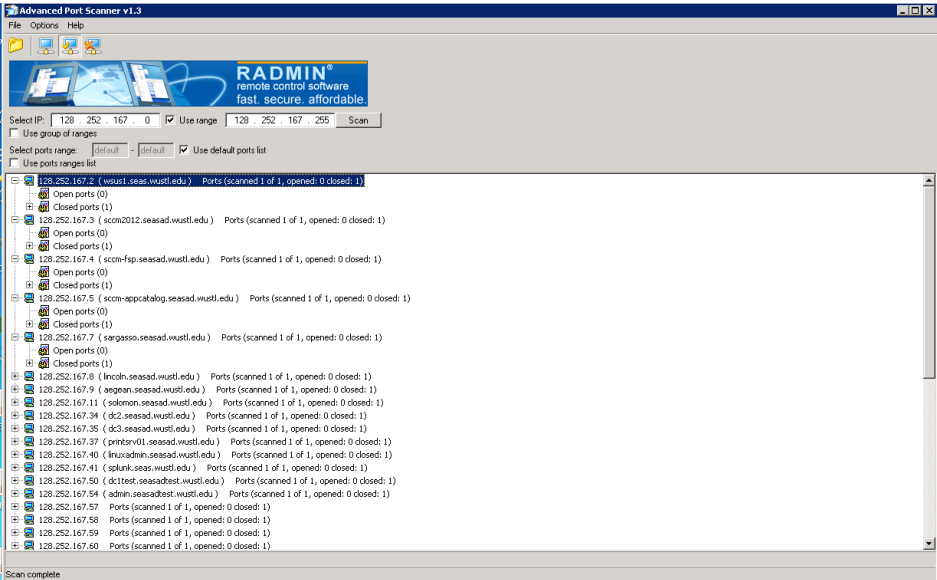


Network Security Lab 2

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 (0.0000s latency)
```

```
Host is up (0.000s 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:45:07:75:35 (Sony)
Nmap scan report for 192.168.1.6
Host is up (0.017s latency).
MAC Address: C0:8D:01:B2:B4:BB (Samsung Electro Mechanics)
Nmap scan report for 192.168.1.9
Host is up (0.027s latency).
MAC Address: BB:27:EB:96:42:18 (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.10
Host is up (0.027s latency).
MAC Address: BB:27:EB:41:47:32 (Raspberry Pi Foundation)
Nmap scan report for rp10 (192.168.1.11)
Host is up (0.038s latency).
MAC Address: BB:27:EB:57:C0:8F (Raspberry Pi Foundation)
Nmap scan report for rp13 (192.168.1.15)
Host is up (-0.067s latency).
MAC Address: BB:27:EB:A0:08:BB (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.18
Host is up (-0.085s latency).
MAC Address: 90:B6:06:16:13:24 (Murata Manufacturing)

Nmap scan report for 192.168.1.118
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 17020ms
rtt min/avg/max/mdev = 13.157/14.961/23.761/2.427 ms
david@yogata:~/Downloads$
```

The screenshot displays a dual-monitor setup. The left monitor shows a web browser with the Washington University in St. Louis homepage. The right monitor shows the Wireshark network traffic capture interface, displaying a list of captured packets and their details.

**Washington University in St. Louis**

Academics Research Campus Experience Who We Are

A PLACE where people matter and serious work is done

for PROSPECTIVE STUDENTS for CURRENT STUDENTS for PARENTS & FAMILIES for FACULTY & STAFF for ALUMNI & FRIENDS

**Wireshark**

Capturing from any (host 128.252.114.30)

No.	Time	Source	Destination	Protocol	Length	Info
1991	38.481198910	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2033297 Win=65535
1992	38.482182986	128.252.114.30	192.168.1.2	TCP	4412	[TCP segment of a reassembled PDU]
1993	38.482195426	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2037641 Win=65535
1994	38.482207688	128.252.114.30	192.168.1.2	TLSv1.2	4412	Application Data
1995	38.482230952	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2041985 Win=65535
1996	38.483079927	128.252.114.30	192.168.1.2	TCP	7308	[TCP segment of a reassembled PDU]
1997	38.483159743	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2049225 Win=65535
1998	38.484312552	128.252.114.30	192.168.1.2	TLSv1.2	5860	Application Data
1999	38.484333465	128.252.114.30	192.168.1.2	TCP	2964	[TCP segment of a reassembled PDU]
2000	38.484344205	128.252.114.30	192.168.1.2	TCP	4412	[TCP segment of a reassembled PDU]
2001	38.484428480	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2062257 Win=65535
2002	38.485026319	128.252.114.30	192.168.1.2	TLSv1.2	4412	Application Data
2003	38.485045335	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2066681 Win=65535
2004	38.487434534	128.252.114.30	192.168.1.2	TCP	1516	[TCP segment of a reassembled PDU]
2005	38.488245189	128.252.114.30	192.168.1.2	TCP	1516	[TCP segment of a reassembled PDU]
2006	38.488261129	128.252.114.30	192.168.1.2	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2069497 Win=65535
2007	38.488277566	128.252.114.30	192.168.1.2	TCP	2964	[TCP segment of a reassembled PDU]
2008	38.488282759	128.252.114.30	192.168.1.2	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2072393 Win=65535
2009	38.488287292	128.252.114.30	192.168.1.2	TCP	1516	[TCP segment of a reassembled PDU]
2010	38.488910818	128.252.114.30	192.168.1.2	TLSv1.2	2765	Application Data
2011	38.488929635	128.252.114.30	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2076538 Win=65535
2012	38.515402160	192.168.1.2	128.252.114.30	TLSv1.2	713	Application Data
2013	38.534593291	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [ACK] Seq=2076538 Ack=4941 Win=9320
2014	38.535991939	128.252.114.30	192.168.1.2	TCP	1516	[TCP segment of a reassembled PDU]
2015	38.536832237	128.252.114.30	192.168.1.2	TLSv1.2	113	Application Data
2016	38.536847161	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4941 Ack=2078031 Win=65535
2017	38.536862564	128.252.114.30	192.168.1.2	TLSv1.2	1561	Application Data
2018	38.536869275	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4296 Ack=2079524 Win=65535
2019	38.536880525	128.252.114.30	192.168.1.2	TCP	4412	[TCP segment of a reassembled PDU]
2020	38.536887362	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4941 Ack=2083868 Win=65535
2021	38.537738146	128.252.114.30	192.168.1.2	TLSv1.2	8289	Application Data
2022	38.537779319	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4941 Ack=2092089 Win=65535
2023	42.923223118	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [FIN, ACK] Seq=409530 Ack=9296 Win=0
2024	42.923202182	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [FIN, ACK] Seq=506728 Ack=4893 Win=0
2025	42.923873832	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [FIN, ACK] Seq=429954 Ack=4968 Win=0
2026	42.923895593	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [FIN, ACK] Seq=432947 Ack=4248 Win=0
2027	42.931687651	128.252.114.30	192.168.1.2	TCP	68	68 443 → 43086 [FIN, ACK] Seq=504762 Ack=6263 Win=0
2028	42.962822809	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4248 Ack=432948 Win=65535
2029	42.962871365	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4968 Ack=429955 Win=65535
2030	42.962898059	192.168.1.2	128.252.114.30	TCP	68	68 43086 → 443 [ACK] Seq=4893 Ack=506729 Win=65535



# 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=409531 Win=65535

2032 42.970707357 192.168.1.2 128.252.114.30 TCP 68 43090 → 443 [ACK] Seq=9293 Ack=504763 Win=65535

2033 43.749742359 128.252.114.30 192.168.1.2 TCP 68 443 → 43088 [FIN, ACK] Seq=2092089 Ack=4941 Win=65535

2034 43.782671946 192.168.1.2 128.252.114.30 TCP 68 43086 → 443 [ACK] Seq=4941 Ack=2092090 Win=65535

2035 43.80059192 192.168.1.2 128.252.114.30 TCP 68 43086 → 443 [ACK] Seq=4941 Ack=2092090 Win=65535

2036 81.891262425 128.252.114.30 192.168.1.2 TCP 68 [TCP Window Update] 80 → 40884 [ACK] Seq=111 Ack=40884

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..4.10.0.s....

0020 00 fc 72 1e a8 4e 01 bb 54 1b 01 c4 eb ae cf 64 ..F..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