EEw382N Security Laboratory 5 Report

Student: Mark DiValerio (mad2799)
Professor: Mohit Tiwari
TA: Austin Harris
Department of Electrical & Computer Engineering
The University of Texas at Austin

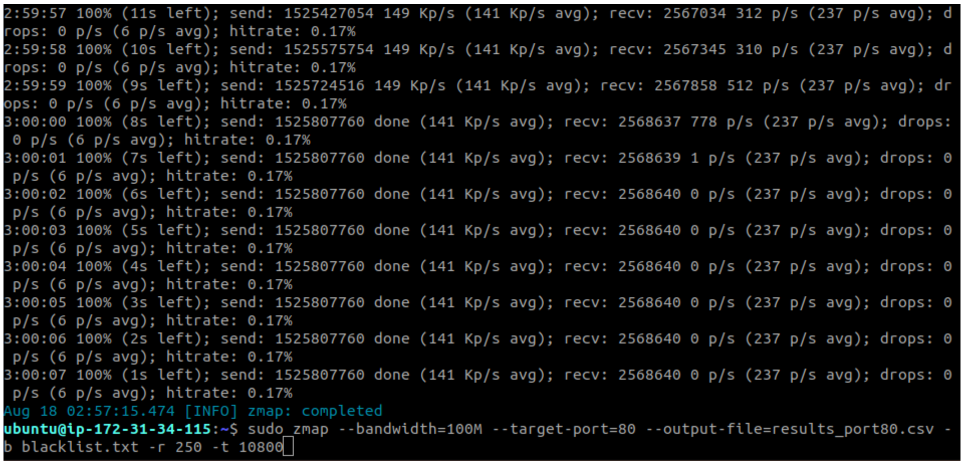
August 20, 2019

1 Part 1 - Scanning the Internet

In this part of the lab, I scanned the internet on port 80 to see what I could find. Using an AWS EC2 c5.12xlarge instance with 12 Gbps network to alleviate the bandwidth bottleneck, I ran the zmap command:

```
sudo zmap --bandwidth=100M --target-port=80 --output-file=results_port80.csv
-b blacklist.txt -r 250 -t 10800
```

You can see the terminal output from the command in the screenshot below in Figure 1. After three hours, the `part1/aws-large-results/zmap-large-ips-port80.csv` contained over 2.5 million IP addresses. I then grouped the IPs by network as you can see in the referenced file (submitted with this report) in `part1/aws-large-results/raw-ip-grouping-port80.csv`. A statistical analysis of the network is represented in Figure 2.



```
2:59:57 100% (11s left); send: 1525427054 149 Kp/s (141 Kp/s avg); recv: 2567034 312 p/s (237 p/s avg); d
rops: 0 p/s (6 p/s avg); hitrate: 0.17%
2:59:58 100% (10s left); send: 1525575754 149 Kp/s (141 Kp/s avg); recv: 2567345 310 p/s (237 p/s avg); d
rops: 0 p/s (6 p/s avg); hitrate: 0.17%
2:59:59 100% (9s left); send: 1525724516 149 Kp/s (141 Kp/s avg); recv: 2567858 512 p/s (237 p/s avg); dr
ops: 0 p/s (6 p/s avg); hitrate: 0.17%
3:00:00 100% (8s left); send: 1525807760 done (141 Kp/s avg); recv: 2568637 778 p/s (237 p/s avg); drops:
 0 p/s (6 p/s avg); hitrate: 0.17%
3:00:01 100% (7s left); send: 1525807760 done (141 Kp/s avg); recv: 2568639 1 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:02 100% (6s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:03 100% (5s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:04 100% (4s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:05 100% (3s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:06 100% (2s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
3:00:07 100% (1s left); send: 1525807760 done (141 Kp/s avg); recv: 2568640 0 p/s (237 p/s avg); drops: 0
 p/s (6 p/s avg); hitrate: 0.17%
Aug 18 02:57:15.474 [INFO] zmap: completed
ubuntu@ip-172-31-34-115:~$ sudo zmap --bandwidth=100M --target-port=80 --output-file=results_port80.csv -
b blacklist.txt -r 250 -t 10800
```

Figure 1: `zmap` Terminal Output

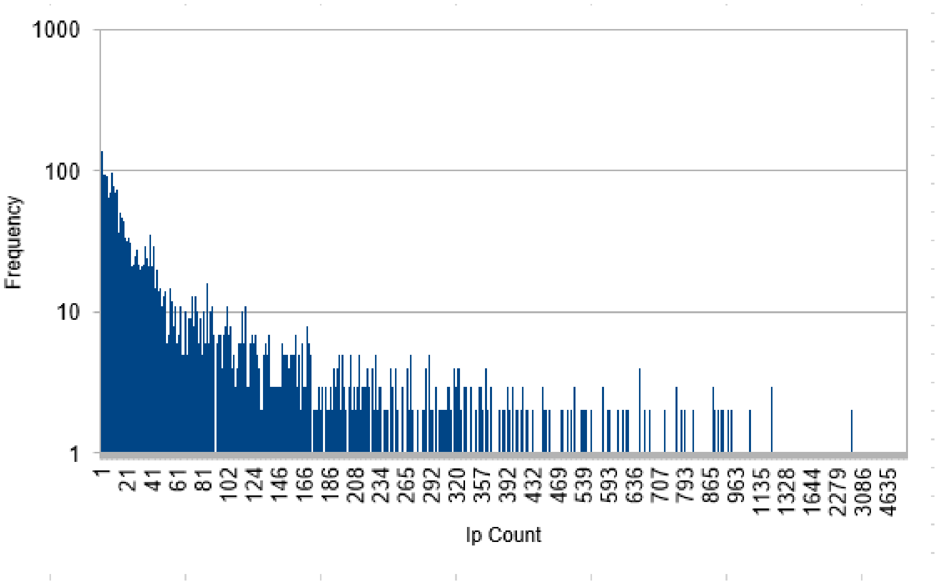


Figure 2: The Number of IPs a Network has and their Frequency of Occurrence

After that, I performed a `whois` command on the top 20 networks that contained the most IP addresses. The `whois` on the first IP address (with the largest network), `185.244.244.114`, revealed that it was a representation of all IP addresses, ranging between `0.0.0.0 - 255.255.255.255` for any unallocated IP. You can see the rest of my `whois` results in `part1/aws-large-results/top-20-whois.txt`. They are primarily internet providers, Cloud, or Web Service companies such as Amazon, Google, and Akamai.

Once I had enough IP addresses, I wrote code to call `whois` and to test if the address was pingable. Of the 8,596 IP Addresses I was able to test, about 70 percent were pingable as shown in Figure 3 below. Further detail about the owner of the addresses can be seen in `part1/aws-large-results/pingable-and-owners.xlsx`.

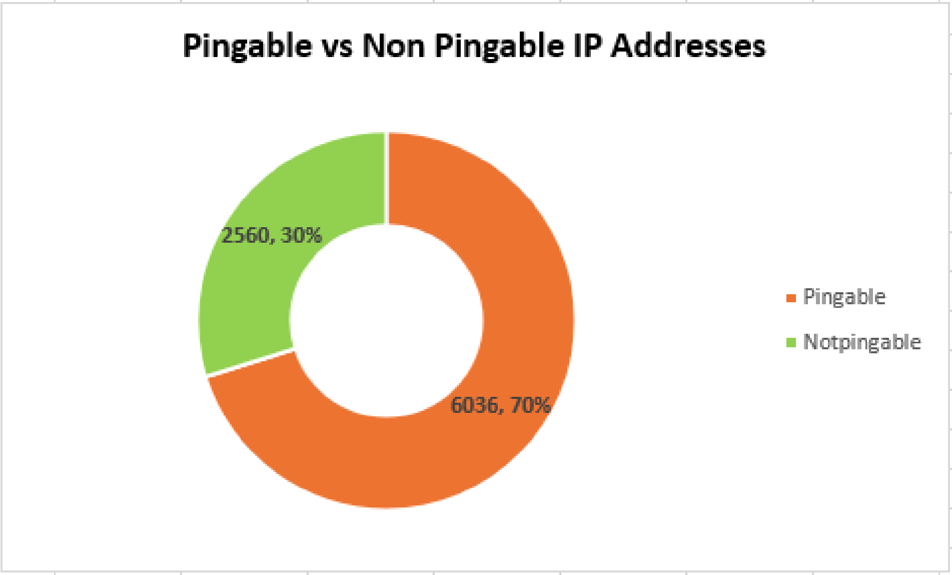
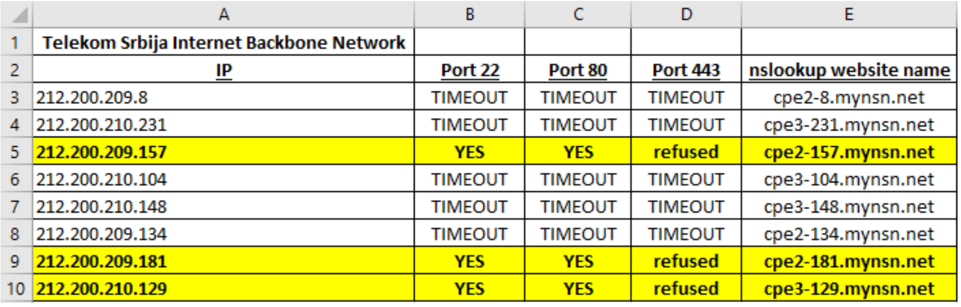


Figure 3: Pingable vs Not Pingable

Finally, I chose a random network to carry out a more in-depth investigation. I selected a smaller network, `212.200.209.8`, that contains eight IPs in total. I attempted to access and connect to each one on port 22, 80, and port 443. Of the eight IP addresses, only three of which I was able to connect via port 22 and port 80, while port 443 the connection did not time out, but it was refused. A summary of these results are represented in Figure 4. My single attempt to SSH into port 22 or visit the websites (listed from the `whois` command) met with a password authentication block* and a page not loading, respectively for the ports (*Did not attempt to access or break in). My investigation showed that the IP Address belonged to Media Art Computers and the network I selected is described as the "Telekom Srbija Internet Backbone Network". You can see my whois results in the screenshot in Figure 4 below.



	A	B	C	D	E
1	**Telekom Srbija Internet Backbone Network**				
2	**IP**	**Port 22**	**Port 80**	**Port 443**	**nslookup website name**
3	212.200.209.8	TIMEOUT	TIMEOUT	TIMEOUT	cpe2-8.mynsn.net
4	212.200.210.231	TIMEOUT	TIMEOUT	TIMEOUT	cpe3-231.mynsn.net
5	**212.200.209.157**	**YES**	**YES**	**refused**	**cpe2-157.mynsn.net**
6	212.200.210.104	TIMEOUT	TIMEOUT	TIMEOUT	cpe3-104.mynsn.net
7	212.200.210.148	TIMEOUT	TIMEOUT	TIMEOUT	cpe3-148.mynsn.net
8	212.200.209.134	TIMEOUT	TIMEOUT	TIMEOUT	cpe2-134.mynsn.net
9	**212.200.209.181**	**YES**	**YES**	**refused**	**cpe2-181.mynsn.net**
10	**212.200.210.129**	**YES**	**YES**	**refused**	**cpe3-129.mynsn.net**

Figure 4: Random Network `212.200.209.8` Analysis

2 Part 2 - Packet Visibility: BRO, VPN, TOR

In Part 2 of this lab, I recorded accessing ten websites, ten times each using three different connection methods for a total of 300 captured pcap files: “BRO” for using a regular (Firefox) browser under normal connections, “VPN” for regular browser while on a VPN connection, and “TOR” for using a Tor browser on a normal connection (not VPN). During each access I performed a `CTRL+Shift+R` to hard-refresh so cached static content would not vary my network packets (as I would load all the cached files again) and this report’s statistics. You can see all 300 pcap files in `part2/` directory submitted with this lab.

A statistical analysis was performed on the ten websites where average packet size and packets sent count were graphed. The data was extracted using `tcpdump` and the Wireshark application (Statistic/Packet Lengths menu). These results are located in the `part2/all_stats` file location, each site’s analysis is saved as an excel file. A sample of these results for the cat website is represented in Figure 5 and 6.

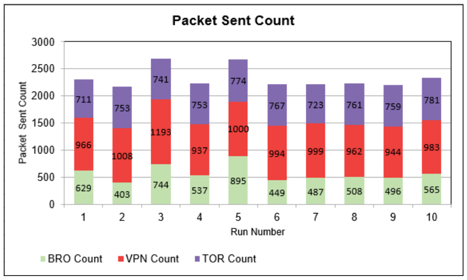


Figure 5: Packet Sent Count - Cat

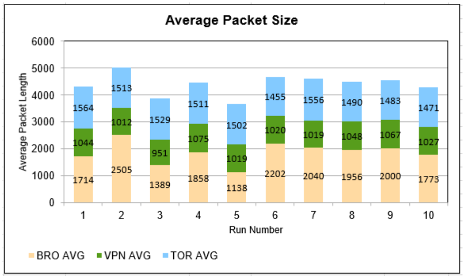
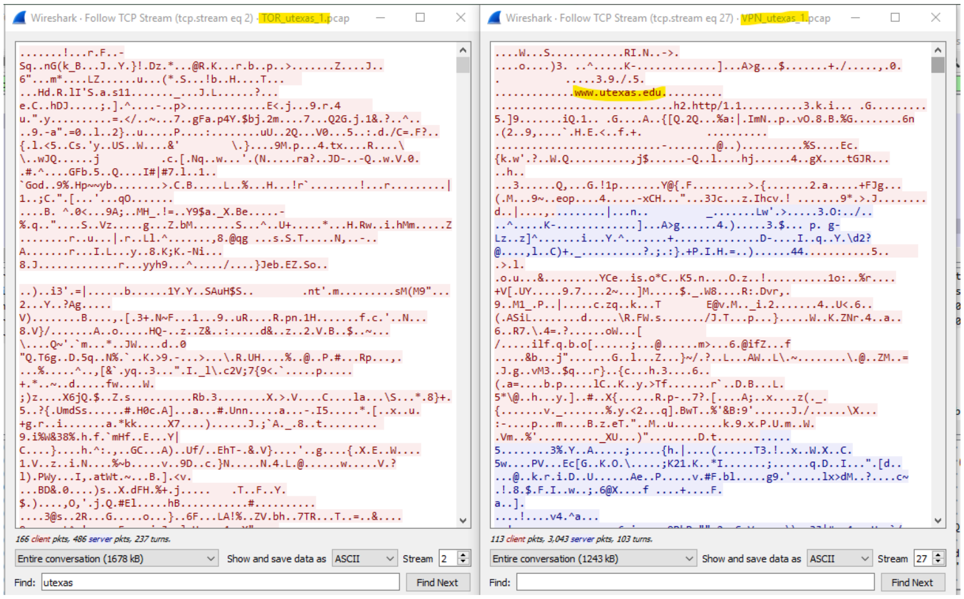


Figure 6: Average Packet Size - Cat

One interesting thing I discovered when evaluating the recordings was that VPN packets have a maximum length of 1514 bytes. This is the maximum length of a single packet but packets are normally strung together. Because I was using a VPN, only individual packets are evaluated.

For VPN, I was able to identify the destination location easily by following the TCP (utexas) trace, however the same method did not work for the TOR packets as you can see in the highlighted sections in Figure 7 below.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · TOR_utexas_1.pcap

```
.......!...r.F..-
Sq..nG(k_B...J..Y.}!.Dz.*...@R.K...r.b..p..>.......Z....J..
6"...m*....LZ......u...(*.S...!b..H....T...
...Hd.R.lI'S.a.s11......_...J.L......?...
e.C..hDJ.....;.].^....-..p>............E<.j...9.r.4
u.".y..........=.</..~...7..gFa.p4Y.$bj.2m....7...Q2G.j.1&.?..^..
..9.-a".=0..1..2}..u.....P....:........uU..2Q...V0...5..:.d./C=.F?..
{.l.<5..Cs.'y..US..W....&'        \.}....9M.p...4.tx....R....\
\..wJQ......j          .c.[.Nq..w...'.(N.....ra?..JD-..-Q..w.V.0.
.#.^....GFb.5..Q....I#|#7.l..1..
`God..9%.Hp~~yb........>.C.B.....L..%...H...!r`........!...r.........|
1..;C.".[...'...qO.......
....B. ^.0<...9A;..MH_.!=..Y9$a._X.Be.....-
%.q.."....S..Vz.....g...Z.bM.......S...^..U+.....*...H.Rw..i.hMm.....Z
........r..u...|.r..Ll.^.......,8.@qg ...s.S.T.....N,..-..
A.......r...I.L...y..8.K;K.-Ni...
8.J.............r...yyh9...^...../....}Jeb.EZ.So..

..)..i3'.=|......b......1Y.Y..SAuH$S..       .nt'.m.........sM(M9"...
2...Y..?Ag.....
V)........B....,.[.3+.N~F...1...9..uR....R.pn.1H.......f.c.'..N...
8.V}/.......A..o.....HQ-..z..Z&..:.....d&..z..2.V.B..$..~...
\....Q~'.`m...*..JW....d..0
"Q.T6g..D.5q..N%.`..K.>9.-...>...\.R.UH....%..@..P.#...Rp...,.
...%.....^..,[&`.yq..3...".I._l\.c2V;7{9<.`.....p.....
+.*..~..d.....fw....W.
;)z....X6jQ.$..Z.s..........Rb.3........X.>.V....C....la...\S...*.8}+.
5..?{.UmdSs......#.H0c.A]...a...#.Unn.....a...-.I5.....*.[..x..u.
+g.r..i.......a.*kk.....X7....).....J.;`A._.8..t.........
9.i%W&38%.h.f.`mHf..E...Y|
C....}....h.^:.,..GC...A)..Uf/..EhT-.&.V}....'..g....{.X.E..W....
1.V..z..i.N....%~b.....v..9D..c.}N.....N.4.L.@......w.....V.?
l).PWy...I,.atWt.~...B.].<v.
...BD&.0....)s..X.dFH.%+.j.....   .T..F..Y.
$.)....,O,'.j.Q.#El.....hB...........#.........
....3@s..2R...G.....o...}..6F...LA!%..ZV.bh..7TR...T..=..&....
```

166 client pkts, 486 server pkts, 237 turns.

Entire conversation (1678 kB) Show and save data as ASCII Stream 2

Find: utexas

Wireshark · Follow TCP Stream (tcp.stream eq 27) · VPN_utexas_1.pcap

```
....W...S............RI.N..->.
....o....)3. ..^.....K-.............]...A>g...$.......+./.....,.0.
.          .....3.9./.5.
.............www.utexas.edu..........
..............................h2.http/1.1..........3.k.i... .G.........
5.]9.......iQ.1.. .G....A..{[Q.2Q...%a:|.ImN..p..vO.8.B.%G........6n
.(2..9,....`.H.E.<..f.+.          ..........
............................-........@..)..........%S....Ec.
{k.w'.?..W.Q..........,j$......-Q..l....hj......4..gX....tGJR...
..h..
...3......Q,...G.!1p.......Y@{.F.........>.{.......2.a.....+FJg...
(.M...9~..eop....4.....-xCH..."...3Jc...z.Ihcv.! .......9*.>.J........
d..|....,........|...n..        _.......Lw'.>.....3.O:../..
..^.....K-.............]...A>g......4.).....3.$... p. g-
Lz..z]^.......i...Y.^.......+.............D-....I..q..Y.\d2?
@....,l..C)+._..........?.;.:}.+P.I.H.=..)......44...........5..
.>.l.
.o.u...&.........YCe..is.o*C..K5.n....O.z..!..........1o:..%r....
+V[.UY.....9.7....2~...]M.....$._.W8....R:.Dvr,.
9..M1_.P..|.....c.zq..k...T       E@v.M.._i.2.......4..U<.6..
(.ASiL........d.....\R.FW.s......./J.T...p...}.....W..K.ZNr.4..a..
6..R7.\.4=.?......oW...[
/.....ilf.q.b.o[......;...@......m>...6.@ifZ...f
.....&b...j"......G..l...Z...}~/.?..L...AW..L\.~........\.@..ZM..=
.J.g..vM3..$q...r}..{c...h.3....6..
(.a=....b.p.....lC..K..y.>Tf.......r`..D.B...L.
5*\@..h...y.]..#..X{......R.p-..7?.[....A;..x....z(._.
{.......v._.......%.y.<2...q].BwT..%'&B:9'......J./......\X...
:-....p...m....B.z.eT."..M..u........k.9.x.P.U.m..W.
.Vm..%'.........._XU...)".......D.t............
5........3%.Y..A.....;.....{h.|....(......T3.!..x..W.X..C.
5w....PV...Ec[G..K.O.\.....;K21.K..*I.......;......q.D..I...".[d..
...@..k.r.i.D..U......Ae..P.....v.#F.bl.....g9.'.....1x>dM..?....c~
.!.8.$.F.I..w..;.6@X....f ....+....F.
a..].
....!....v4.^a...
```

113 client pkts, 3,043 server pkts, 103 turns.

Entire conversation (1243 kB) Show and save data as ASCII Stream 27

Find:

Figure 7: Left is TOR, Right is VPN

3 Conclusion

In conclusion, this lab was interesting to investigate and scan the vast IP addresses around the world, learning the network tools, and the differences between TOR and VPN. Creating statistical analyses of each gave me insight into how the packets are made and what they look like. My only feedback for this lab was the time constraint. Scanning enough IP addresses for a report and performing analysis on 300 pcap files made each minute precious, although I understand since it is the summer semester and we only have so much time.