Part 3: Charting a DDOS Attack

Thomas Reid Zuk

March 12, 2016

https://github.com/Freakazoidile/SRT_Assignment_Graphs/tree/master/Part3

Phase 1. The Scan

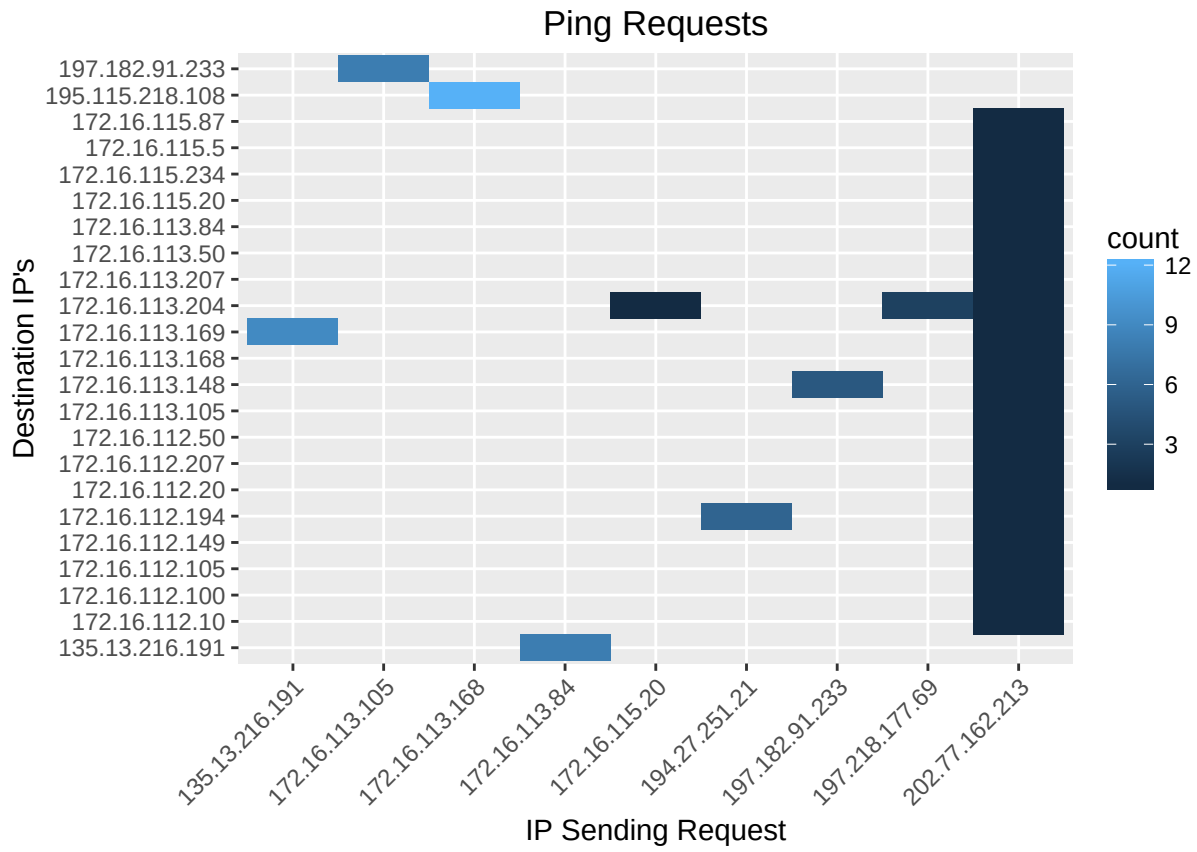
This is a continuous Bivariate Distribution that has been applied to a pcap filtered to show pings on the network.The first part of the attack was a scan of networks:

- 172.16.115.0/24
- 172.16.114.0/24
- 172.16.113.0/24
- 172.16.112.0/24

```
pingsGrouped <- group_by(pings, grepl("* request *",pings$Info))

pingsSet <- subset(pingsGrouped, pingsGrouped[ ,8] == TRUE, drop = TRUE)

ggplot(pingsSet, aes(pingsSet$Source,pingsSet$Destination)) +
  geom_bin2d() +
  ylab("Destination IP's") +
  xlab("IP Sending Request") +
  ggtitle("Ping Requests")  +
  theme(axis.text.x = element_text(angle = 45, hjust = 1))
```



The large vertical bar along the right hand side represents a host scanning the network. A single IP as Source correlated to Destinations show the destinations are part of the networks listed. The count of these requests is extremely like compared to most other occurences of pings on the network. This helps to illustrate that it was a scan, a simple request once over a period of time. There are not many hosts that generated the requests, and most of the other hosts have higher count of ICMP pings.

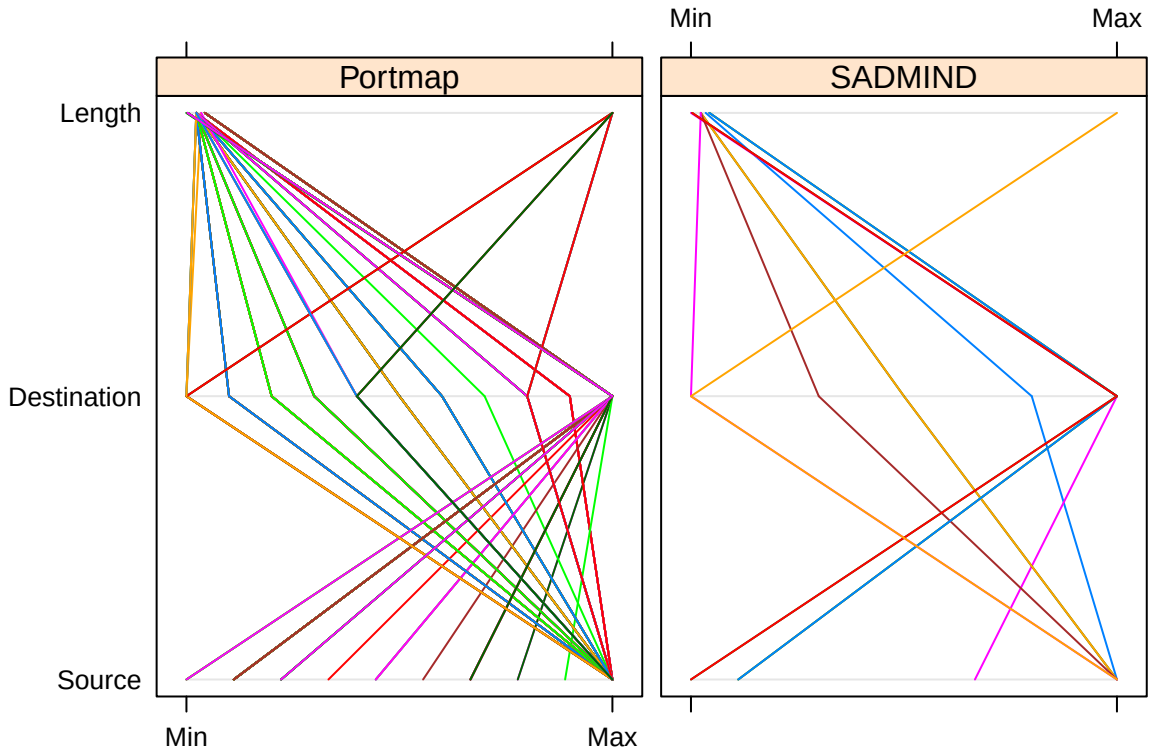
Phase 2. Probe for sadmind

```
rpcLess <- read.csv('rpcLess.csv', header = TRUE)
rpc_filtered <- read.csv('rpc_filtered.csv', header = TRUE)

rpc_less <- select(rpcLess, Source, Destination, Length)
rpcScan <- subset(rpcLess, (Length < 1400))

newRpc <- select(rpc_filtered, Source, Destination, Length)

parallelplot(~newRpc[1:3] | Protocol, rpcScan)
```



This graph shows by Source IP (represented by the Min and Max) which host sends traffic to Destination devices, and the length of the packet sent. The graph is further separated by Portmap and SADMIND protocols

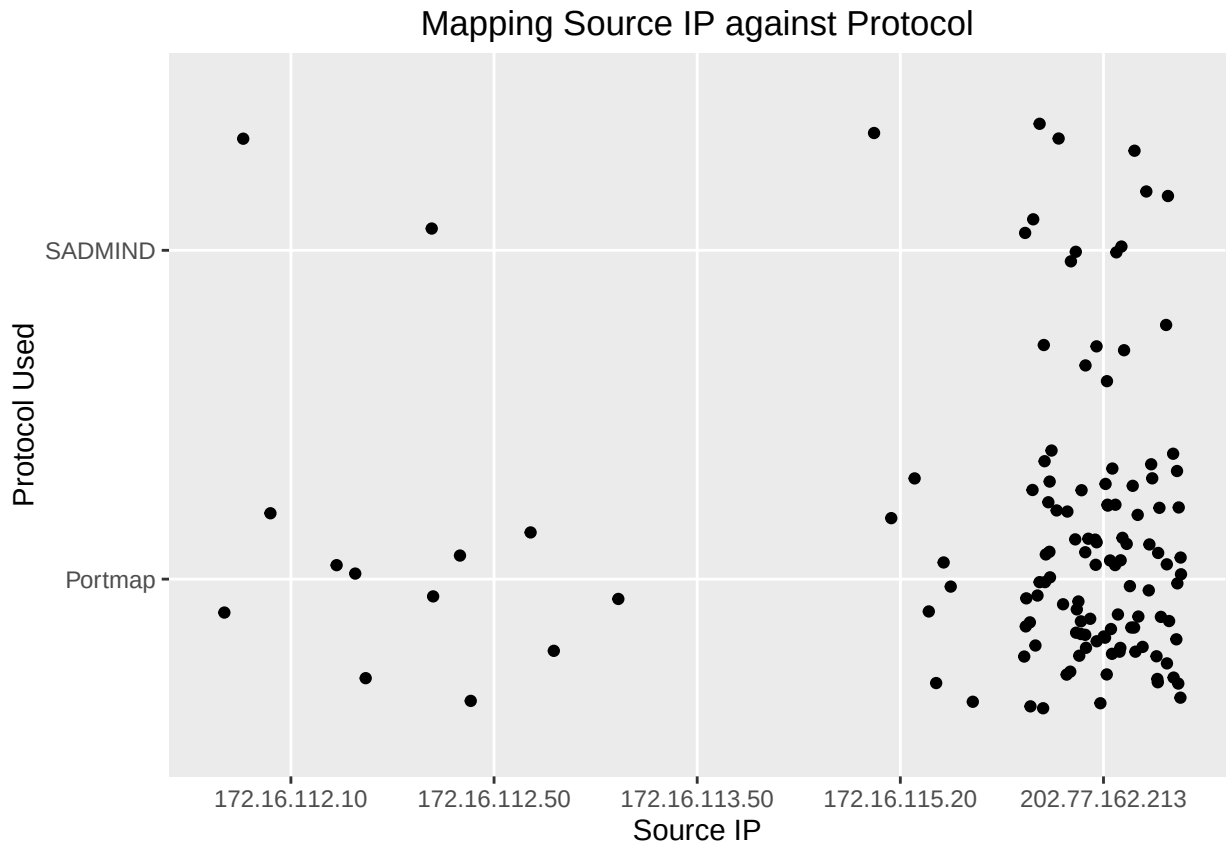
Both Portmap and SADMIND visualizations show a single IP connecting to many different IP's, while the rest of the IP's only send traffic to a single IP. The single IP is the attacker sending a SADMING Ping function to probe the hosts, and then using the response to connect to the machines.

Having many other IP's all connecting to a single IP with both sADMIND and Portmap protocols that the attacker does not have any traffic between is an indication they are logging into a central system they are familiar with.

Phase 3. Breaking into the Targets

```
rcp_tn <- read.csv('rpcLess.csv', header = TRUE)

ggplot(rcp_tn, aes(Source, Protocol)) +
  geom_jitter() +
  ylab("Protocol Used") +
  xlab("Source IP") +
  ggtitle("Mapping Source IP against Protocol")
```

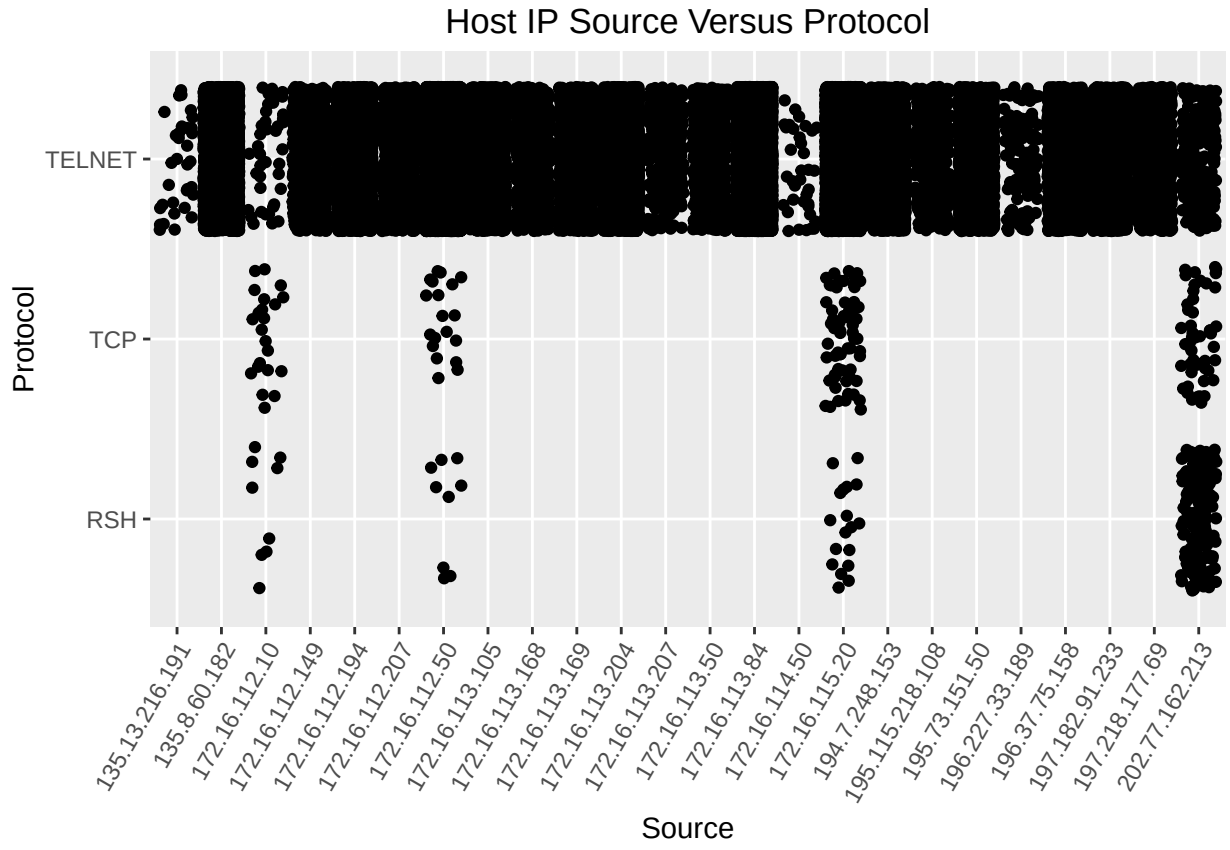


This graph clearly shows an abnormally high amount of traffic relating to protocols that SADMIND vulnerbaility traffic would use coming from a single host. The other Source IP's of traffic all belong to the networks which are subject to the attack. The other hosts have very little traffic compared to the external IP's single traffic.

Phase 4. Installing Software

```
tcp_trsh <- read.csv('tcp_trsh', header = TRUE)

ggplot(tcp_trsh, aes(Source, Protocol)) +
  geom_jitter() +
  ggtitle("Host IP Source Versus Protocol")  +
  theme(axis.text.x = element_text(angle = 60, hjust = 1))
```



In this phase of the attack Telnet sessions were started to connect to the target machines which created a directory. RCP (Remote Copy) was used to transfer files to to the targets. RCP uses TCP ports 513 and 514 and are represented on the graph by TCP protocol. The graph illustrates all hosts that use RCP, Telnet, and RSH during the entire pcap session.

Each of hosts were attacked and infected stand out by the use of Telnet, RCP and RSH traffic. The attacker is singled out by having more RSH traffic than any other host, and is one of the few external IP's among the Sources of the traffic.

Part 5. The DDOS Attack

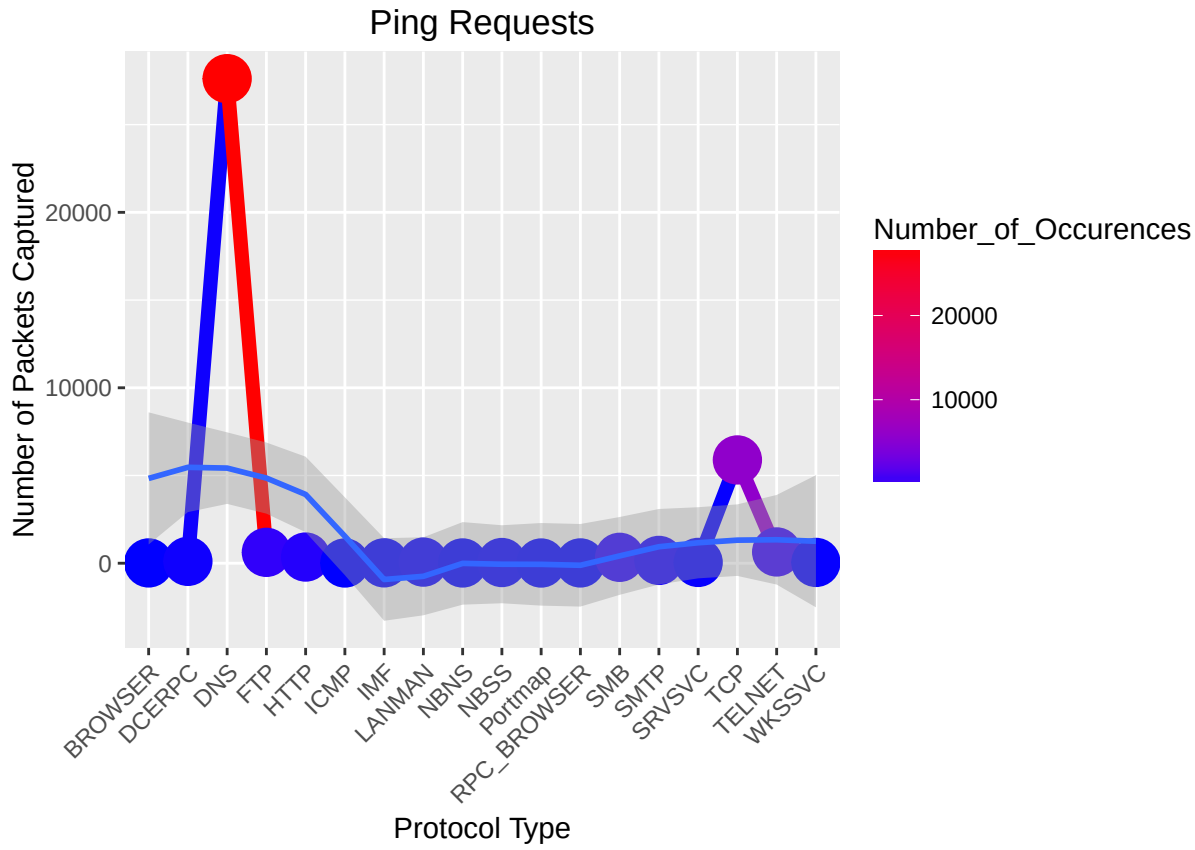
```
rcp_tn <- read.csv('packets', header = TRUE)

attack <- getenum(rcp_tn, 'Protocol', add.n=TRUE, add.freq=TRUE)

colnames(attack) <- c("enum", "Number_of_Occurences", "n", "freq")

ggplot(attack, aes(enum, Number_of_Occurences, group = 1, colour = Number_of_Occurences)) +
  geom_line(size=2.5) +
  geom_point(size=8) +
  stat_smooth(level=0.5) +
  scale_colour_gradient(high="red", low="blue") +
  theme(axis.text.x = element_text(angle = 45, hjust = 1)) +
```

```
  ylab("Number of Packets Captured") +
  xlab("Protocol Type") +
  ggtitle("Ping Requests")
```



This graph shows the amount of traffic by protocol occuring across the entire session of the attack. The fact that there is more DNS traffic within this network that TCP traffic should raise flags

References

http://www.ll.mit.edu/ideval/data/2000/LLS_DDOS_1.0.html

https://cran.r-project.org/web/packages/ips/ips.pdf

https://cran.r-project.org/web/packages/linkcomm/vignettes/linkcomm.pdf

https://rdatamining.wordpress.com/2012/05/17/an-example-of-social-network-analysis-with-r-using-package-igraph/

http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0070.html