Detection of events pertaining to security in the Science DMZ network

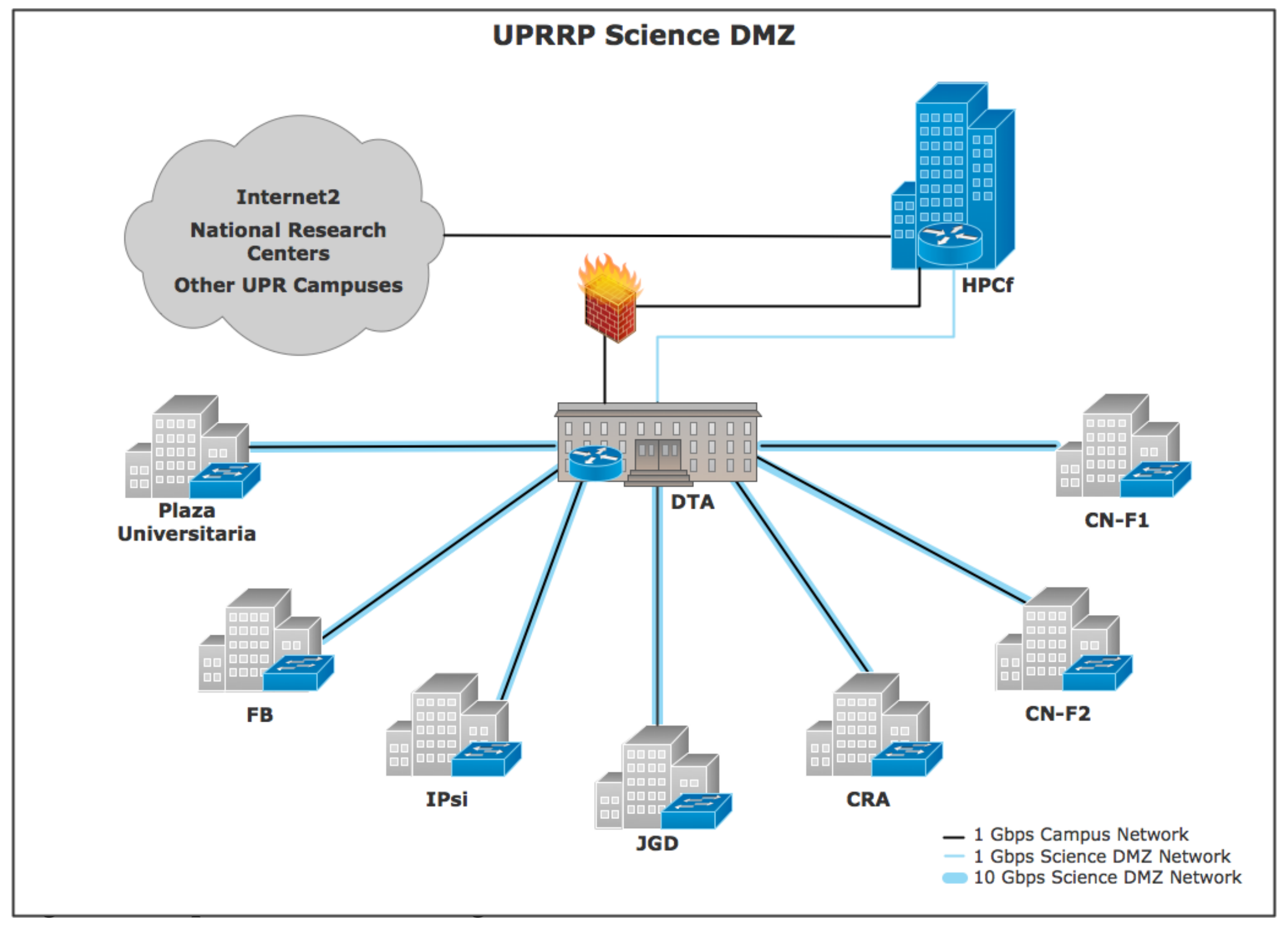
Mariecarmen A. Reynoso Toribio (1), Humberto G. Ortiz-Zuazaga (1,2)
Department of Computer Science, Río Piedras Campus (1), Assistant Professor, University of Puerto Rico (2)

Abstract

The University of Puerto Rico use its network for different type of services like students services, administrative services, and research services. The Computer Science Department is building an independent network known as the Science DMZ (10GE) dedicated to science research and the transference of big data. This Science DMZ is a public network without a firewall, thus the analysis of the traffic in the Science DMZ network will help us to learn efficient ways to protect the network without affecting the data transfers.

Introduction

Science DMZ is a portion of the network, built at or near the campus or laboratory's local network perimeter that is designed such that the equipment, configuration, and security policies are optimized for high-performance scientific applications rather than for general-purpose business systems or "enterprise" computing [1]. But Science DMZ doesn't have a firewall because the primary function of a firewall rule set is to permit or deny network traffic using packet header information in a process where each packet is typically matched against the firewall rule set [2]. But when the data occupies lots of memory, the firewall does not allow the data to pass, and it is not possible to transfer all the data at an efficient rate, and that is the reason why the Science DMZ network can not have a firewall[3]. The problem is that if a network doesn't have a firewall, it is exposed to network vulnerabilities and its protection is very limited[3]



Objective

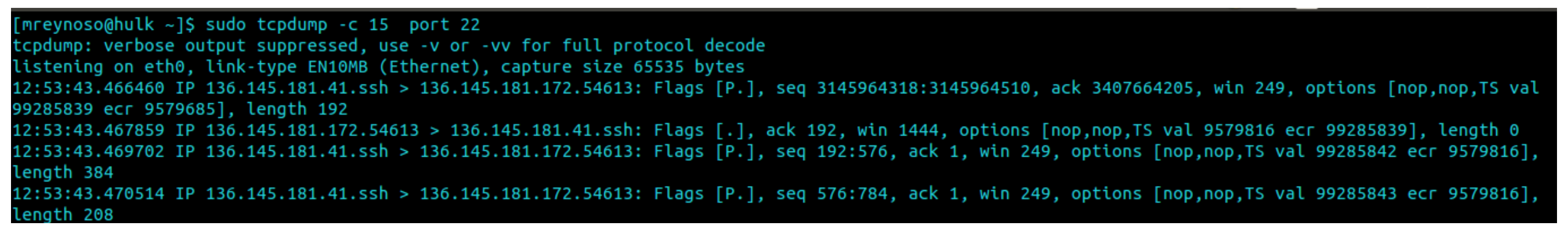
To analyze the network traffic of the Science DMZ to find characteristics that leads to the detection of events to protect the network.

Methodology

We used the Raspberry Pi and we installed TCPDump packet sniffer. We chose to analyze the SSH connections on port 22, specially the TCP connection flags[4][5].

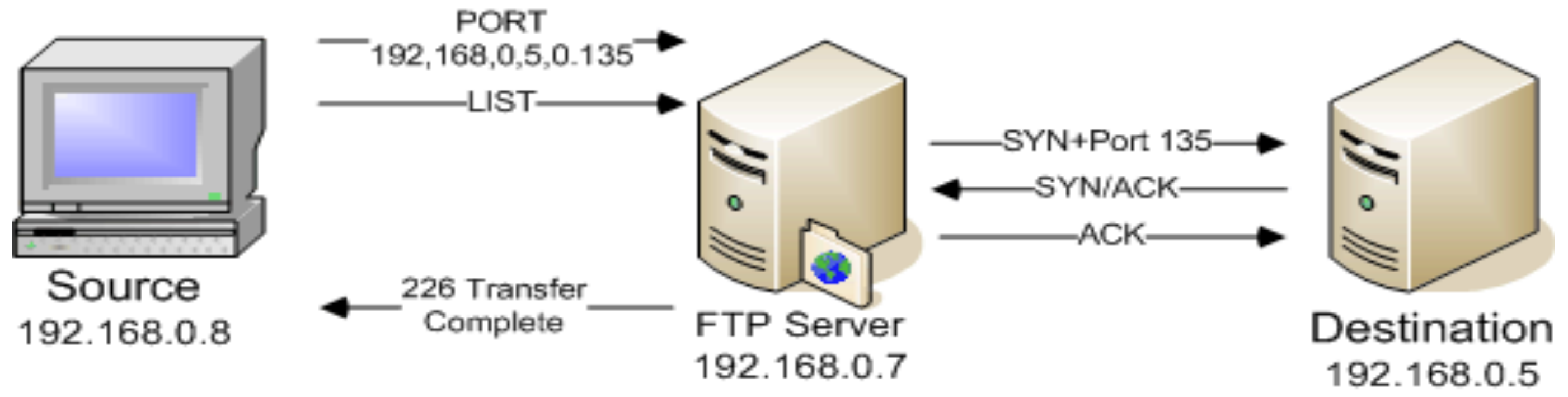
Command for filter the packets in port 22
#tcpdump port 22

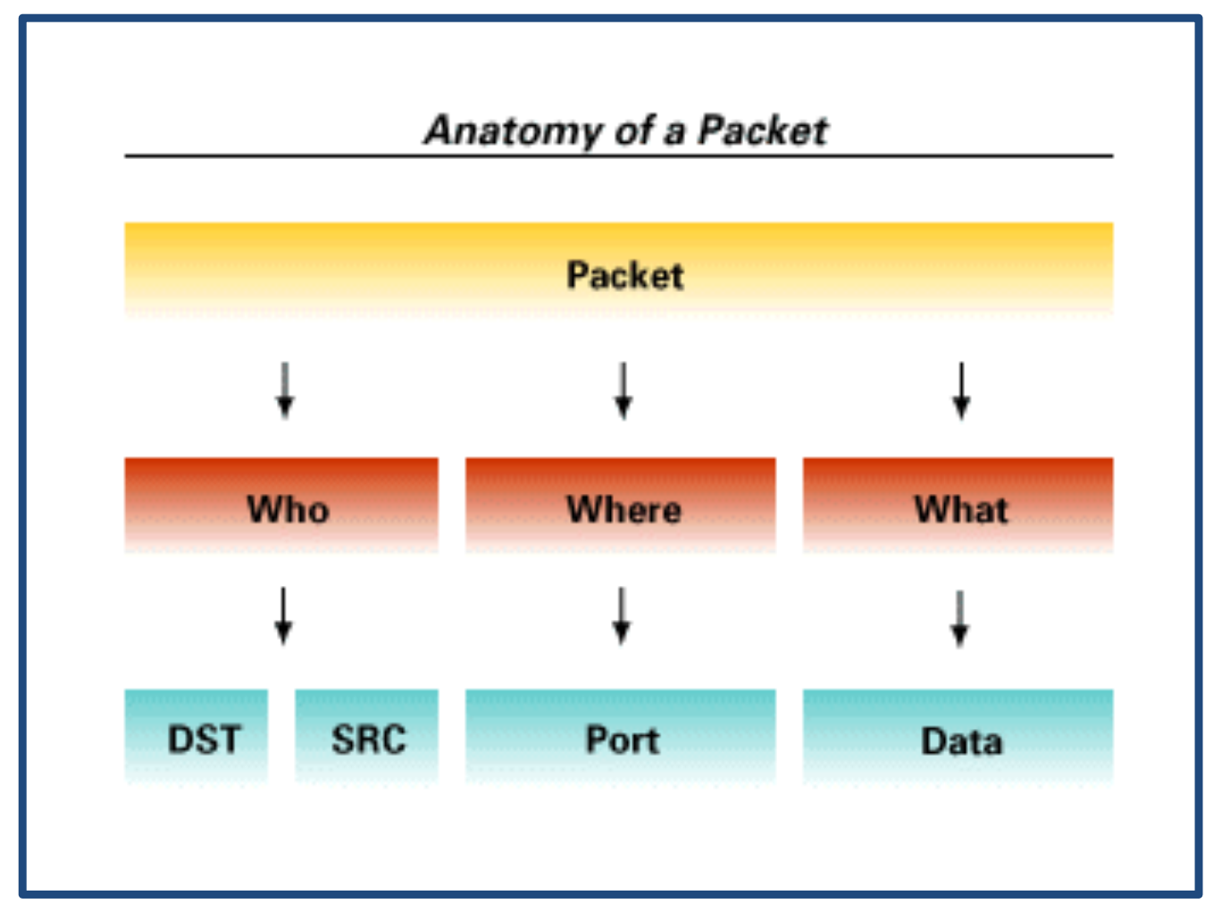
Command for see the connection of the first two packets on port 22
sudo tcpdump port 22 and "tcp[tcpflags] & (tcp-syn)!=0"

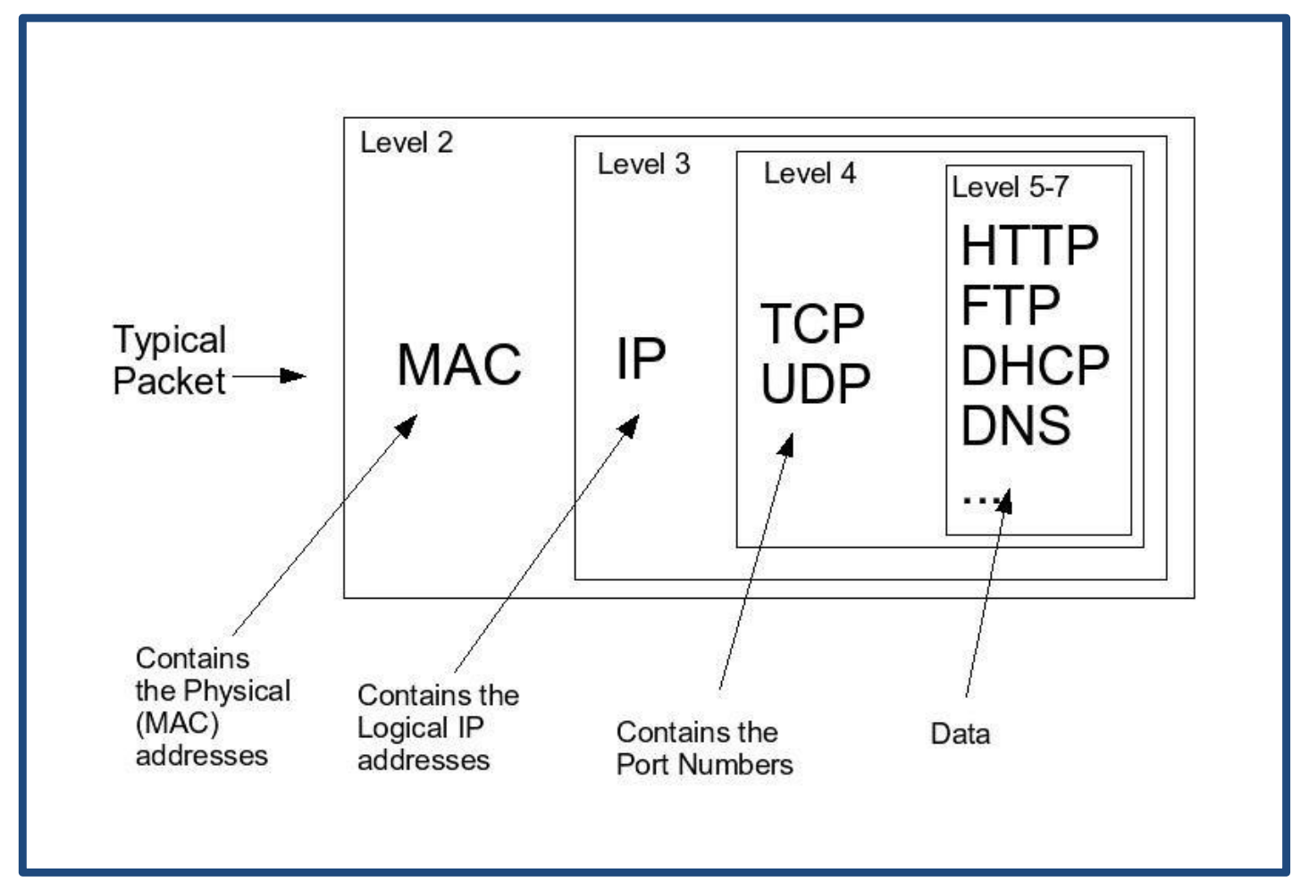


```
[mreynoso@hulk ~]$ sudo tcpdump -c 15  port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:53:43.466460 IP 136.145.181.41.ssh > 136.145.181.172.54613: Flags [P.], seq 3145964318:3145964510, ack 3407664205, win 249, options [nop,nop,TS val
99285839 ecr 9579685], length 192
12:53:43.467859 IP 136.145.181.172.54613 > 136.145.181.41.ssh: Flags [.], ack 192, win 1444, options [nop,nop,TS val 9579816 ecr 99285839], length 0
12:53:43.469702 IP 136.145.181.41.ssh > 136.145.181.172.54613: Flags [P.], seq 192:576, ack 1, win 249, options [nop,nop,TS val 99285842 ecr 9579816],
length 384
12:53:43.470514 IP 136.145.181.41.ssh > 136.145.181.172.54613: Flags [P.], seq 576:784, ack 1, win 249, options [nop,nop,TS val 99285843 ecr 9579816],
length 208
```

Figure 1: Using the command "#tcpdump port 22" in Hulk






Typical Packet
Level 2
MAC
Level 3
IP
Level 4
TCP
UDP
Level 5-7
HTTP
FTP
DHCP
DNS
...
Contains the Physical (MAC) addresses
Contains the Logical IP addresses
Contains the Port Numbers
Data

Results

The first two packets on port 22 have the first part of a TCP connection. In a week we counted 16851 connection fails on SSH. To do this we processed the traffic files with grep and wc on the UNIX terminal.

Future Works

We will use Snort, that is a open source network intrusion prevention system capable of performing real-time traffic analysis and packet logging on IP networks[5], to analyze the traffic in any port. Then we will develop a program to monitor connections that does not interrupt the data transfer.

Conclusion

The Science DMZ has the capacity to facilitate the data transfer of bid data, but since it doesn't have a firewall the user must be careful that their equipment is safe from network vulnerabilities. Using TCPdump we were able to analyze the packets on port 22 and recognize that the first two packets are part of the TCP connection. The analysis of such connections can help us to learn what are the vulnerabilities on the network and how to solve the problem efficiently.

Reference

[1]General information of Science DMZ network "https://fasterdata.es.net/science-dmz"

[2] Information of Science DMZ architecture "https://fasterdata.es.net/science-dmz/science-dmz-architecture/"

[3]Information of firewall and security "https://fasterdata.es.net/science-dmz/science-dmz-security/"

[4]General information of raspberrypi and use "https://raspberrypi.org"

[5] Manual for use tcpdump commands "http://www.alexonlinux.com/tcpdump-for-dummies"

[6]What is Snort? Definition "http://www.webopedia.com/TERM/S/Snort.html"

Acknowledgement

This work is supported by Academics and Training for the Advancement of Cybersecurity Knowledge in Puerto Rico (ATACK-PR), Scholarship for Cybersecurity Excellence.