Report (9) Captured from 06-04-2018 to 20-04-2018

1-Introduction

The first honeypot studies released by Clifford Stoll in 1990, and from April 2008 the Canadian Honeynet chapter was founded at the University of New Brunswick, NB, Canada. UNB is a member of the Honeynet Project, an international non-profit security research organization.

In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally, honeypots essentially turn the tables for Hackers and Computer Security Experts. They consist of a computer, data or a network site that appears to be part of a network, but is isolated, and seems to contain information or a resource that would be of value to attackers.

There are some benefits of having a honeypot:

- Observe hackers in action and learn about their behavior
- Gather intelligence on attack vectors, malware, and exploits. Use that intel to train your IT staff
- Create profiles of hackers that are trying to gain access to your systems
- Improve your security posture
- Waste hackers' time and resources
- Reduced False Positive
- Cost Effective

Our primary objectives are to gain insight into the security threats, vulnerabilities and behavior of the attackers, investigate tactics and practices of the hacker community and share learned lessons with the IT community, appropriate forums in academia and law enforcement in Canada. So, CIC decided to use cutting edge technology to collect a dataset for Honeynet which includes honeypots on the inside and outside of our network.

These reports are generated based on the weekly traffic. For more information and requesting the weekly captured data, please contact us at a.habibi.l@unb.ca.

2- Technical Setup

In the CIC-Honeynet dataset, we have defined a separated network with these services:

- Email Server(SMTP-IMAP)(Mailoney)
- FTP Server(Dianaee)
- SFTP(Cowrie)
- File Server(Dianaee)
- Web Server (Apache:WordPress-MySql)
- SSH(Kippo,Cowrie)
- Http (Dianaee)
- RDP(Rdpy)
- VNC(Vnclowpot)

Inside the network there are 'like' real users. Each user has real behaviors and surfs the Internet based on the above protocols. The web server is accessible to the public and anyone who can see the website. In the inside network, we put **IPCop** firewall at the edge of network and NAT different services for public users. There is a firewall that some ports such as 20, 21, 22, 53, 80, 143, 443 are opened intentionally to capture and absorb attackers behaviours. Also, there are some weak policies for PCs such as setting common passwords. The real generated data on PCs is mirrored through TAPs for capturing and monitoring by TCPDump.

Furthermore, we add WordPress 4.9.4 and MySQL as database to publish some content on the website. The content of website is news and we have formed kind of honeypot inside of the contact form. So, when the bots want to produce spams, we can grab these spams through "Contact Form 7 Honeypot"(Figure 1).

Figure1: Contact Form 7 Honeypot

CIC-honeynet uses T-POT tool outside firewall which is equipped with several tools. T-Pot is based on well-established honeypot daemons which includes IDS and other tools for attack submission.

The idea behind T-Pot is to create a system, which defines the entire TCP network range as well as some important UDP services as a honeypot. It forwards all incoming attack traffic to the best suited honeypot daemons in order to respond and process it. T-Pot includes docker versions of the following honeypots:

- Conpot,
- Cowrie,
- Dionaea,
- Elasticpot,
- Emobility,
- Glastopf,
- Honeytrap,
- Mailoney,
- Rdpy and

- Vnclowpot

Figure 2 demonstrates the network structure of CIC-honeynet and installed security tools. There are two TAPs for capturing network activities. Outside the firewall, there is T-POT which captures the users' activities through external-TAP. Behind the **IPCop** firewall in the internal network, Security Onion has been used to analyse the captured data through internal-TAP. It is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and other security tools.

In the internal network 3 PCs are running the CIC-Benign behaviour generator (an in house developed agent), includes internet surfing, FTP uploading and downloading, and Emailing activities. Also, four servers include Webserver with WordPress and MySQL, Email Server (Postfix), File Server (Openmediavault) and SSH Server have been installed for different common services. We will change our firewall structure to test different brands every month.

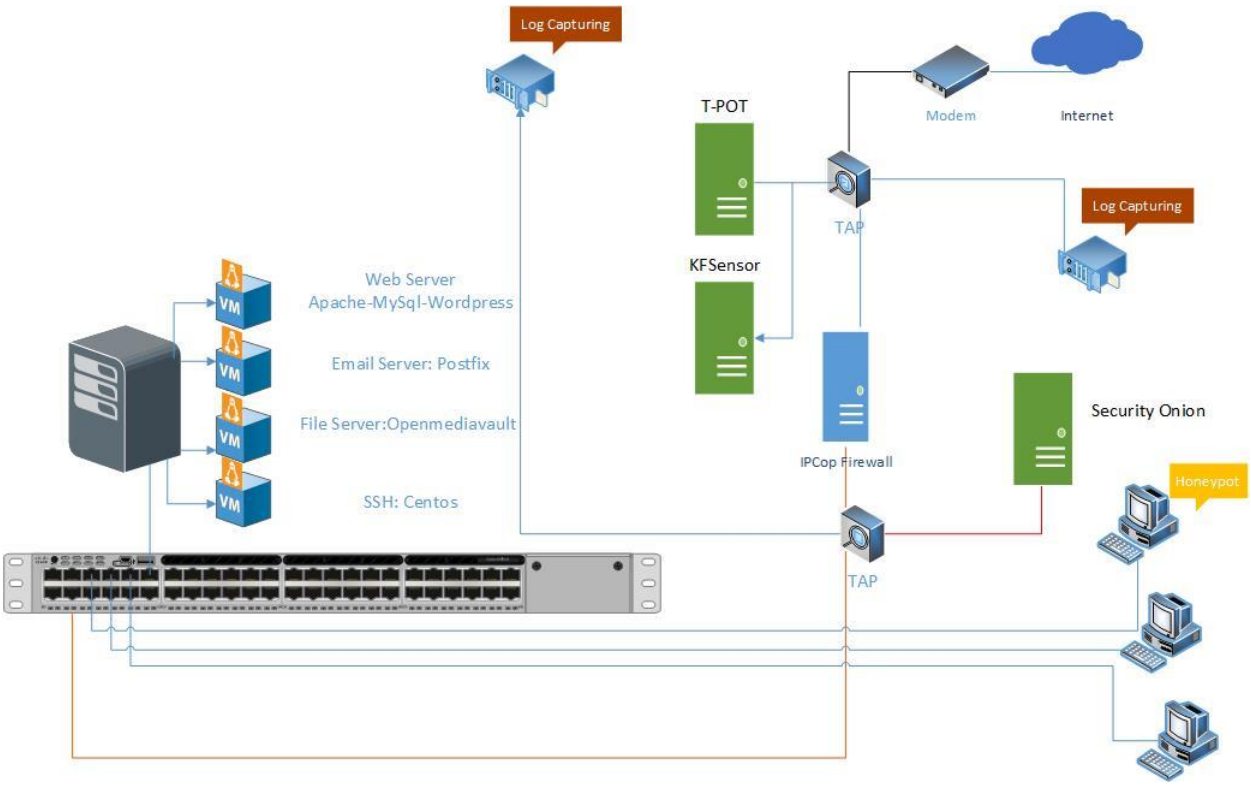


Figure2: Network Diagram

All traffic captured through the internal-TAP and external-TAP and analysis by **CICFlowMeter** which extracts more than 80 traffic features. The source code of CICFlowMeter is available in GitHub.

Also we used **Kippo tools** to mimic the SSH command inside the firewall and captures the users commands. Some easy password such as 1234, 123… are entered in Kippo database to make it vulnerable for attackers.

Furthermore, in this report we used an additional tool KFSensor, which acts as a honeypot, designed to attract and detect hackers' worms and trojans by simulating vulnerable system services. KFSensor is pre-

configured to monitor all TCP and UDP ports, along with ICMP. It is also configured to emulate common services.

3- T-POT Report (External-TAP)

3.1 login attempts

We analyzed the IP addresses that made login attempts using the T-POT. The top ten countries that we recieved login attempts from are listed in Table 1.

Table1: IP breakdown by country

Country	Number of Attack
Russia	1524509
China	158963
United States	75369
Netherlands	26134
Japan	25597
Brazil	24567
Ukraine	16557
Vietnam	13498
Indonesia	6962
Germany	6641

In Table2, top 10 of source IP address and the number of attack are demonstrated.

Table2: Top 10 Source IP

Source IP	Number of Attack
5.188.86.170	944716
109.248.46.113	74465
218.60.67.75	74108
109.248.46.99	72205
109.248.46.71	71589
109.248.46.12	69737
109.248.46.79	69432
61.177.172.97	56350

Source IP	Number of Attack
109.248.46.112	47373

In figure3, top 5 of countries are demonstrated by related ports. For example the attacks from Russia have been 65.41% through port 5900, and 34.4% through port 2222.

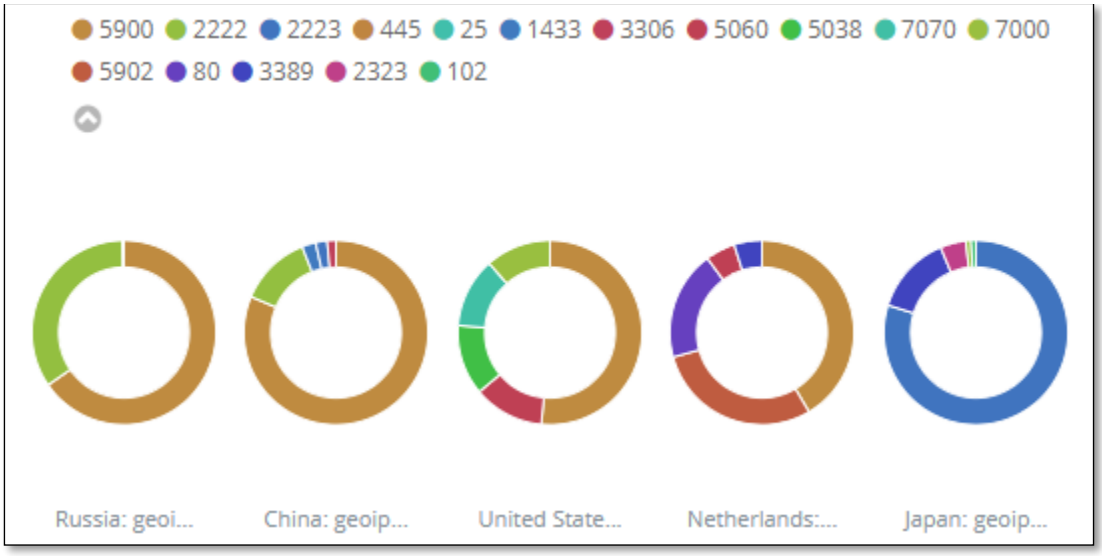


Figure3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

During this week, we had two CVEs namely, CVE-2003-0567 and CVE-2017-0143 which the number of attacks for each CVE are demonstrated in Table3.

Table3: Top 10 Source IP

CVE-ID	Numbers
CVE-2003-0567	28934
CVE-2017-0143	16

The location of attackers based on the IPs presented on Figure 4.

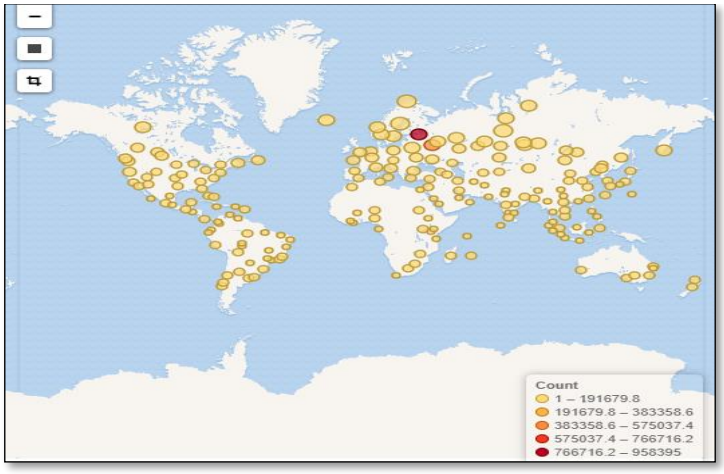


Figure4: The approximate locations of the IP addresses

Based on T-POT, 79.91% of attacks are from addresses with a bad reputation, while only 19.26% are from known attackers (figure5).

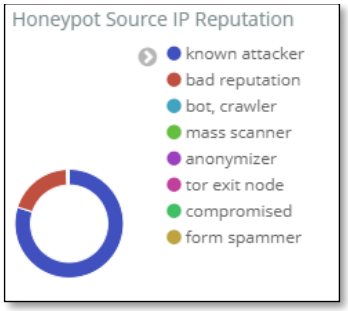


Figure5: External Honeypot source IP Reputation

In Figure 6, some attacks on NGINX webserver have been presented.

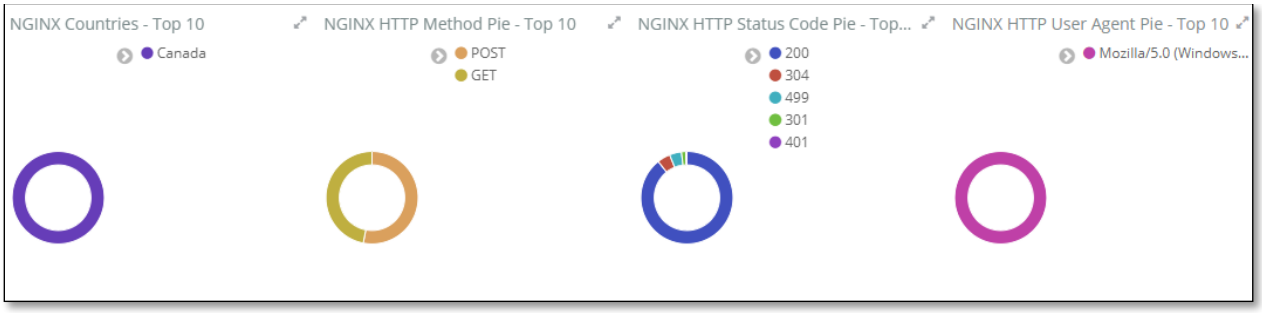


Figure6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4 which around 404801 of them are from Master-Integration Ltd.

Table4: Top 10 Source IP of VNC attack

username	Number of occurrence
109.248.46.113	74465
218.60.67.75	74108
109.248.46.99	72205
109.248.46.71	71589
109.248.46.12	69737
109.248.46.79	69432
109.248.46.112	47373

3.3 TOP Username and password for brute force attack

For brute force attacks, attackers most frequently used the usernames and passwords which are listed in table 5 and 6:

Table5: common username used by attackers

username	Number of occurrence
admin	248872
root	61833
shell	7850
enable	7767
[blank]	1949
guest	1778
default	1448
user	1185
support	1089
supervisor	991

Table6: common password used by attackers

password	Number of occurrence
[blank]	237543
system	7873
sh	7669
1234	2639
admin	2557
12345	2079
password	1849
0	1806
user	1402
123456	1345

3.4 TOP Commands

Table 7 and 8, show the most common commands used by attackers in Cowrie and Mailoney external honeypots. (All commands are available in captured data)

Table7: common command used by attackers grabbed by Cowrie

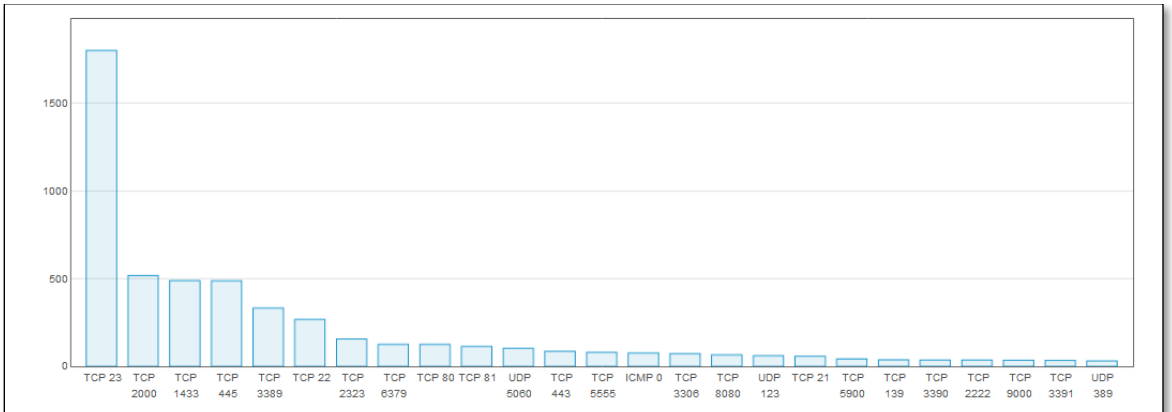
	command	Number of occurrence
1	cat /proc/cpuinfo	138
2	ps -x	138
3	free -m	136
4	export HISTFILE=/dev/null	107
5	export HISTFILESIZE=0	107
6	export HISTSIZE=0	107
7	history -n	107
8	unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH	107

Table8: common command used by attackers grabbed by Mailoney

	command	Number of occurrence
1	EHLO User	1191
2	QUIT	1141
3	AUTH LOGIN	1131
4	HELO mailserver	1107
5	HELO *.*	36
6	STARTTLS	13
7	Ehlo [10.1.10.253]	11
8	EHLO [212.67.215.149]	8
9	EHLO [216.119.103.212]	8
10	Auth Login	4

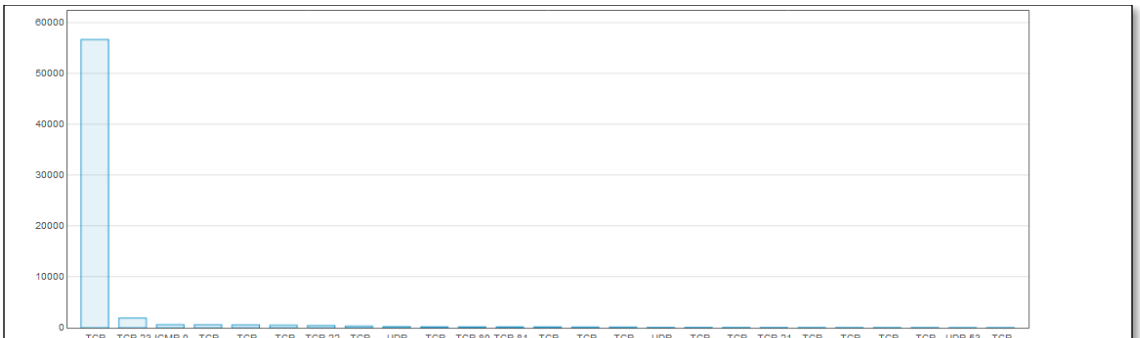
3.5 KFSensor

Figure 7,8, 9 and 10 show the most common attacks in the KFSensor external honeypots**.**



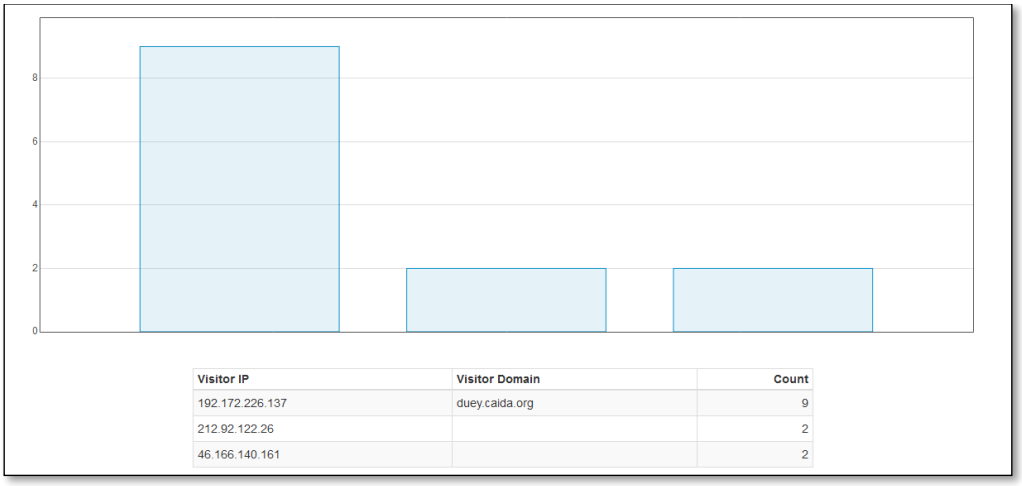
Protocol	Port	Name	Count
TCP	23	Telnet	1801
TCP	2000	iKettle	518
TCP	1433	SQL Server	489
TCP	445	NBT SMB	488
TCP	3389	Terminal Server	333
TCP	22	SSH	268
TCP	2323	Telnet IoT	156
TCP	6379	Redis database	126
TCP	80	IIS	126
TCP	81	IIS 81	114
UDP	5060	SIPS Server	103
TCP	443	IIS HTTPS	87
TCP	5555	ServeMe Trojan	81
ICMP	0	ICMP Echo Request	77
TCP	3306	MySQL Service	73

Figure 7: Top ports by number of visitors



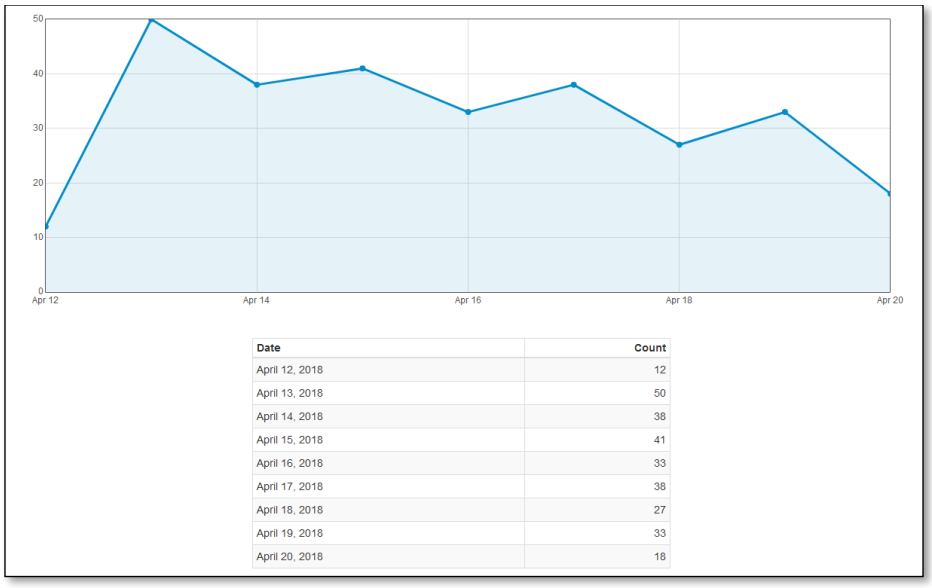
Protocol	Port	Name	Count
TCP	3389	Terminal Server	56602
TCP	23	Telnet	1923
ICMP	0	ICMP Echo Request	631
TCP	1433	SQL Server	619
TCP	445	NBT SMB	583
TCP	2000	iKettle	519
TCP	22	SSH	453
TCP	8545	TCP Syn Scan	332
UDP	5060	SIPS Server	228
TCP	3306	MySQL Service	183
TCP	80	IIS	173
TCP	81	IIS 81	170
TCP	2323	Telnet IoT	167
TCP	6379	Redis database	135
TCP	443	IIS HTTPS	127
UDP	123	Network Time Protocol	85

Figure 8: Top ports by events



Visitor IP	Visitor Domain	Count
192.172.226.137	duey.caida.org	9
212.92.122.26		2
46.166.140.161		2

Figure 9: Top visitors by DOS attacks



Date	Count
April 12, 2018	12
April 13, 2018	50
April 14, 2018	38
April 15, 2018	41
April 16, 2018	33
April 17, 2018	38
April 18, 2018	27
April 19, 2018	33
April 20, 2018	18

Figure 10: Multi-port scan attacks by day

4. Internal Honeypot

As we talked in section2, Inside of our network, **Security Onion** is capturing the number of attacks which is demonstrated in Figure 11. Also we can prove it in Squert and SGUIL which are tools of Security Onion to exactly detect attackers (figure 14, 15, 16). The only difference here is that we intentionally opened some ports on the firewall and when attackers pass the firewall, they face real network. Inside the firewall, as we mentioned in section2, we have 3 PCs and 4 servers for different services. By analysing captured data through Security Onion, we get different result than from section 3.

Count	Value
133	ET DROP Dshield Block Listed Source group 1
34	ET WEB_SERVER Microsoft IIS Remote Code Execution (CVE-2017-7269)
24	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 56
11	ET SCAN Potential SSH Scan
10	ET INFO Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
4	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 35
4	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 75
4	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 87
3	GPL ICMP_INFO PING BSDtype
3	ET DROP Spamhaus DROP Listed Traffic Inbound group 32
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 78
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 60
3	GPL ICMP_INFO PING *NIX
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 3
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 89
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 54
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 79
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 31
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 56
2	ET DROP Spamhaus DROP Listed Traffic Inbound group 13
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 70
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 39
2	ET DROP Spamhaus DROP Listed Traffic Inbound group 31
1	GPL ICMP_INFO PING BayRS Router
1	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 15
1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 84
1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 50
1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 57
1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 51
1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 82

ss=SNORT "-" gr...

Figure11: Traffic requested by users

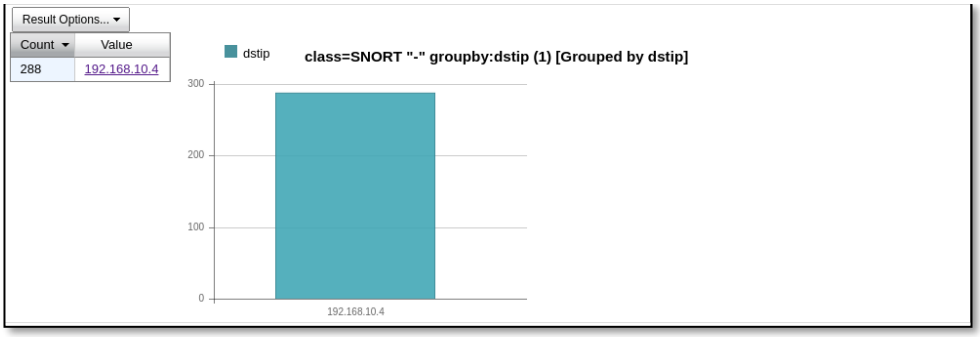


Figure12: users traffic inside network

Inside network, on port 22 we had 5124 attacks which is showcased on Figure 13.

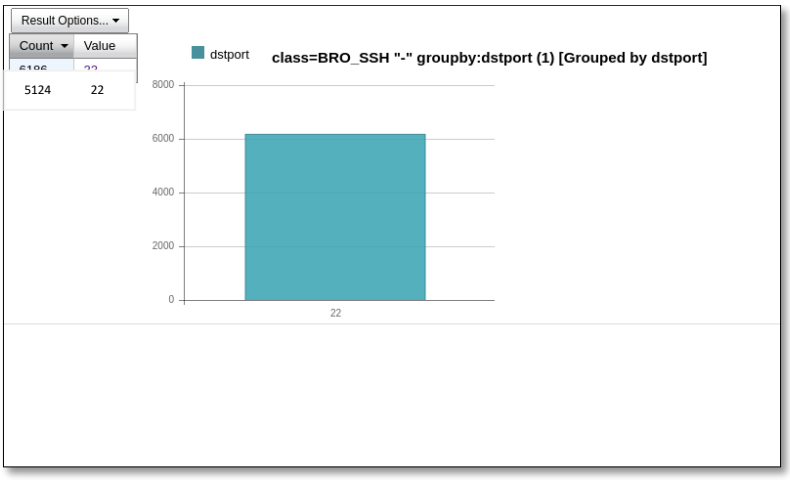


Figure13: Traffic on SSH port

As is mentioned, 14.29 % of what we have seen on the internal honeypot is CVE-2017-7269. We didn't see this kind of attack on the external honeypot (T-POT) (figure 14,15,16).

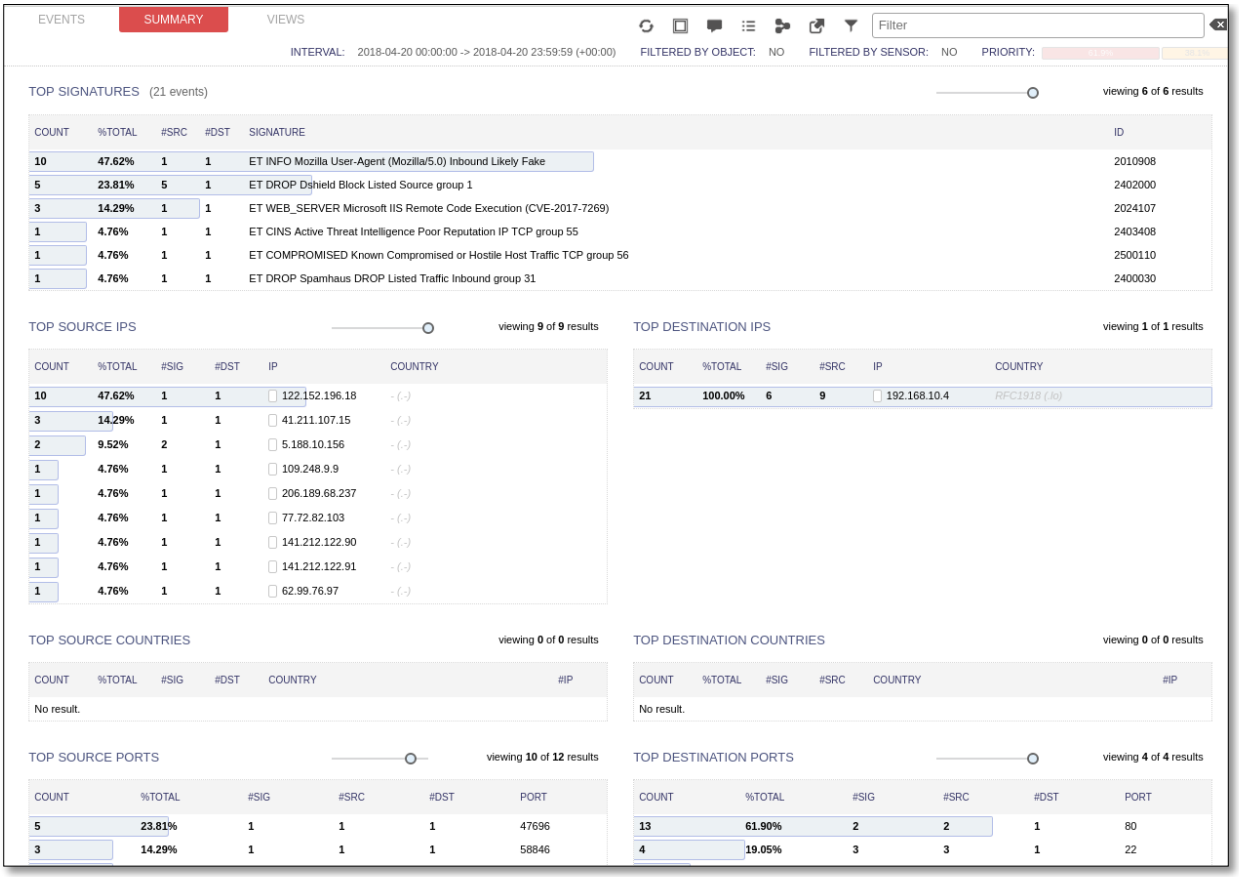


Figure14: Squert summary for attacks

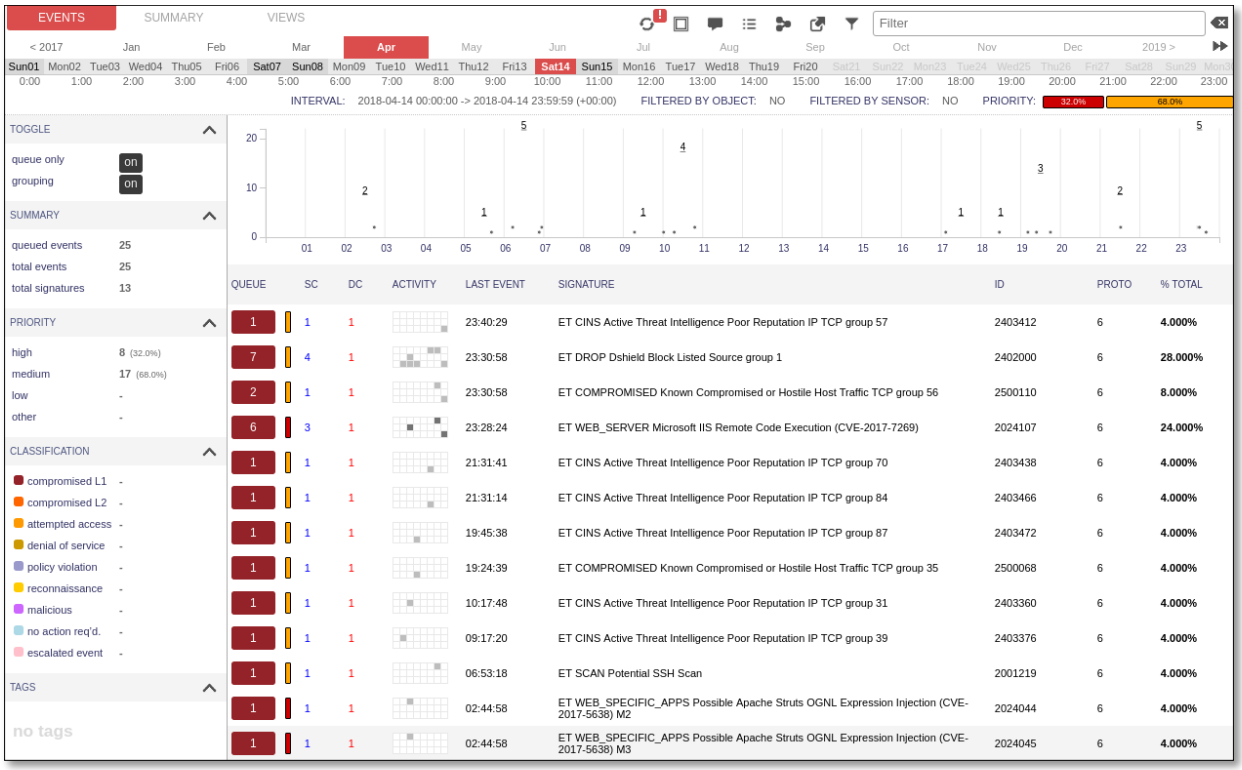


Figure15: Squert shows different attacks on Sat 14th of April

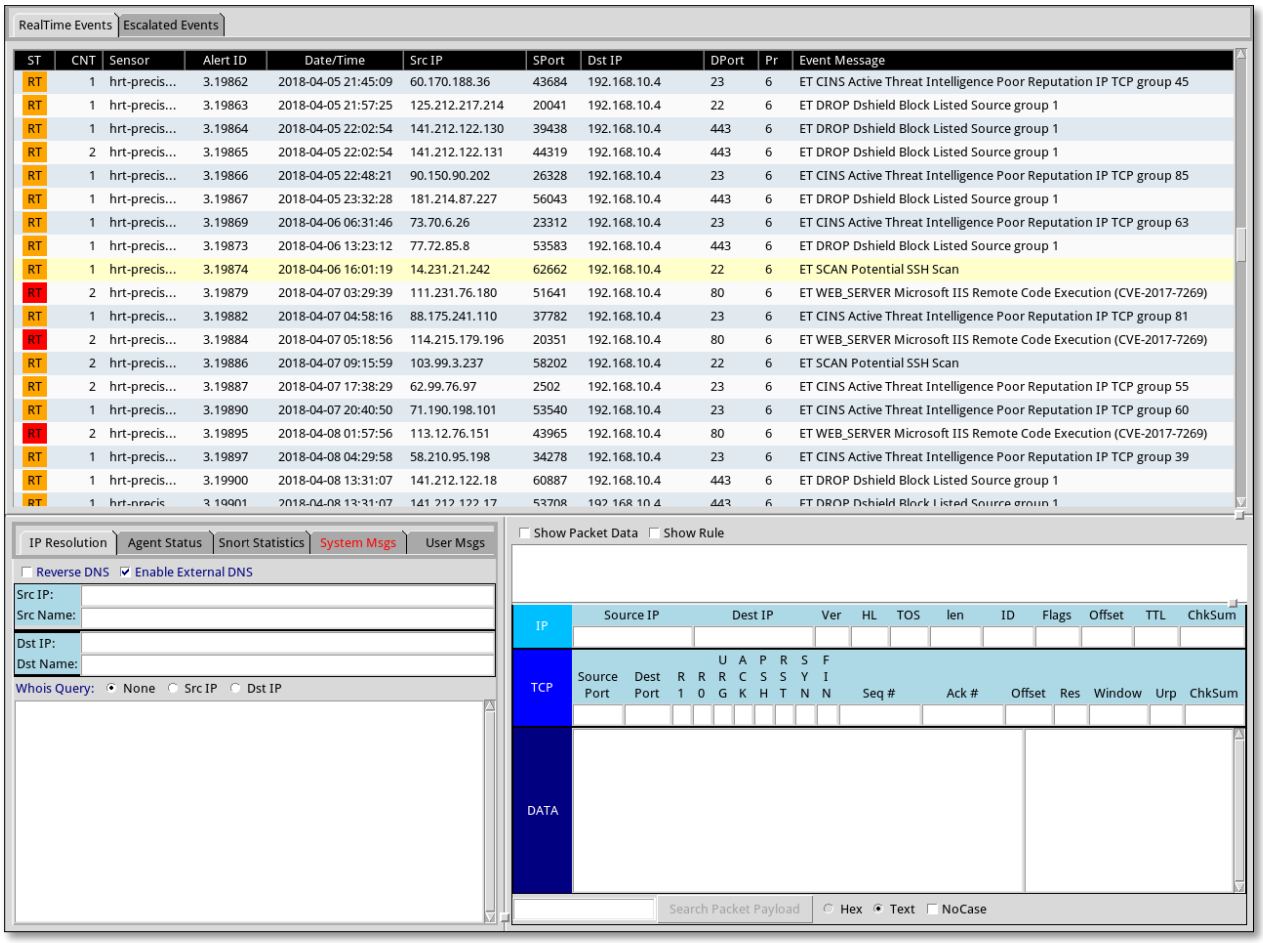


Figure16: attack on SGUIL tools