Report (13) Captured from 01-06-2018 to 15-06-2018

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).

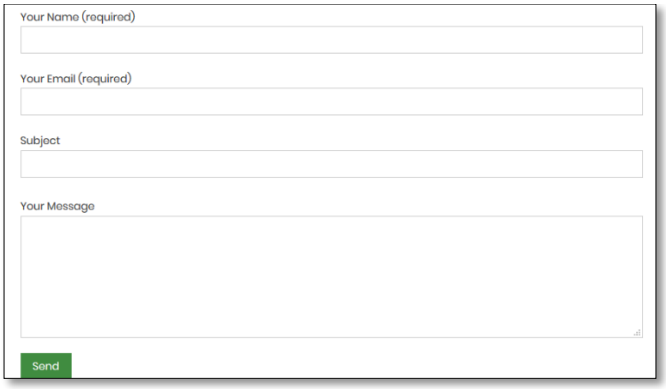

Figure1: Contact Form 7 Honeypot

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.

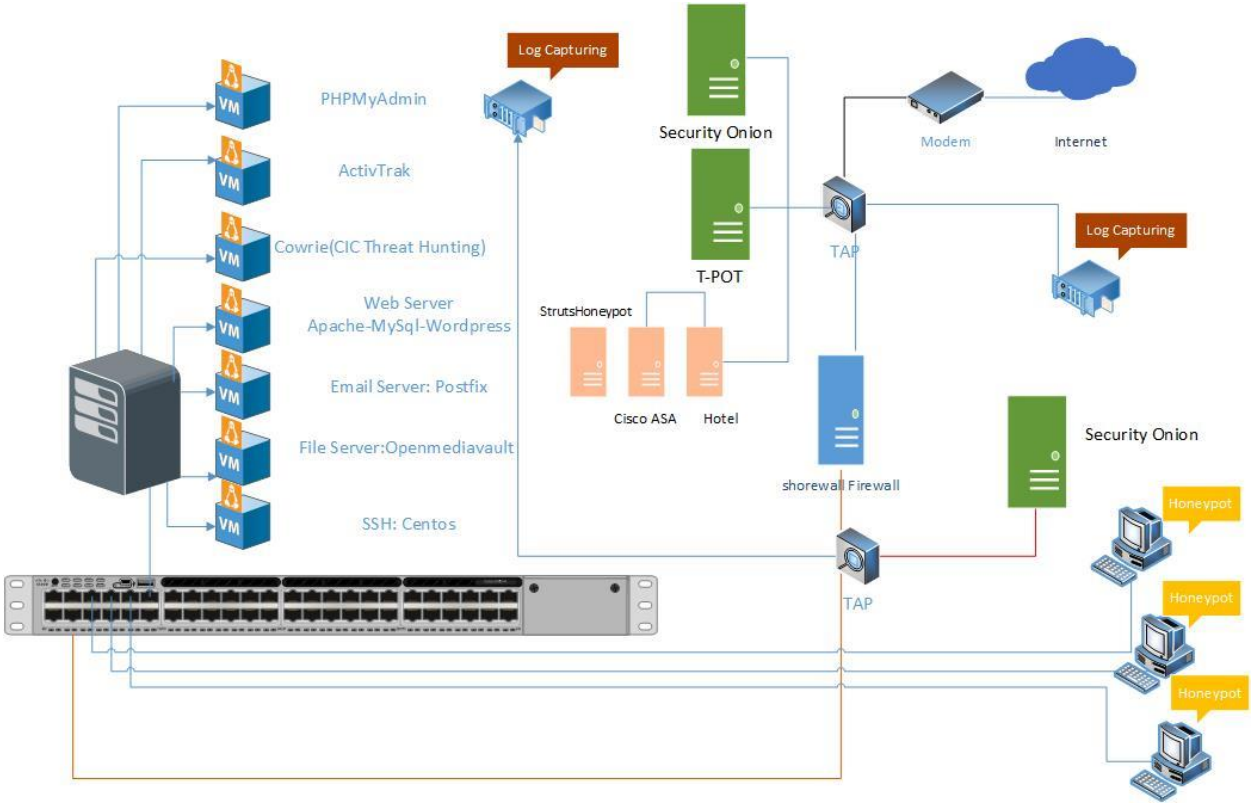

Figure2: Network Diagram

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.

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 ActiveTrack 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
Russia	480911
United States	78132
China	77614
Mexico	56623
Republic of Korea	52386
Ukraine	50832
Brazil	21107
Netherlands	15998
France	14743
Vietnam	12901

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
195.95.151.253	47190
195.201.172.228	34366
109.248.46.113	32347
109.248.46.79	32135
109.248.46.71	32133
109.248.46.99	32128
109.248.46.12	31748
185.156.177.74	28985
167.99.207.50	25105

In figure3, top 5 of countries are demonstrated by related ports. For example, the attacks from the Russia have been 97.89% through port 5900, 1.28% through port 2223.

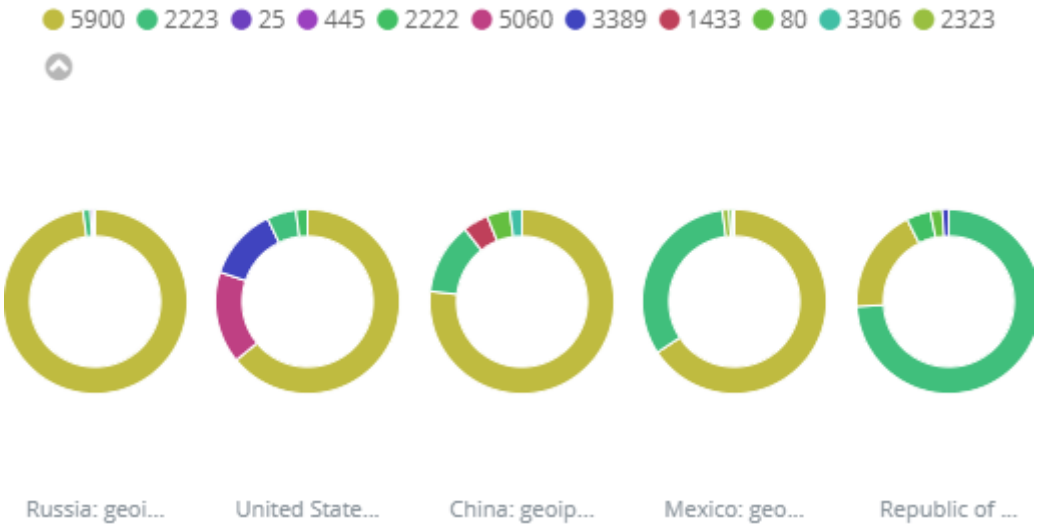

Figure 3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

During this week, we have seen attacks attempt to exploit CVE-2017-0143 14 times.

Table 3: Number of attacks for each CVE

CVE-ID	Numbers
CVE-2017-0143	14

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

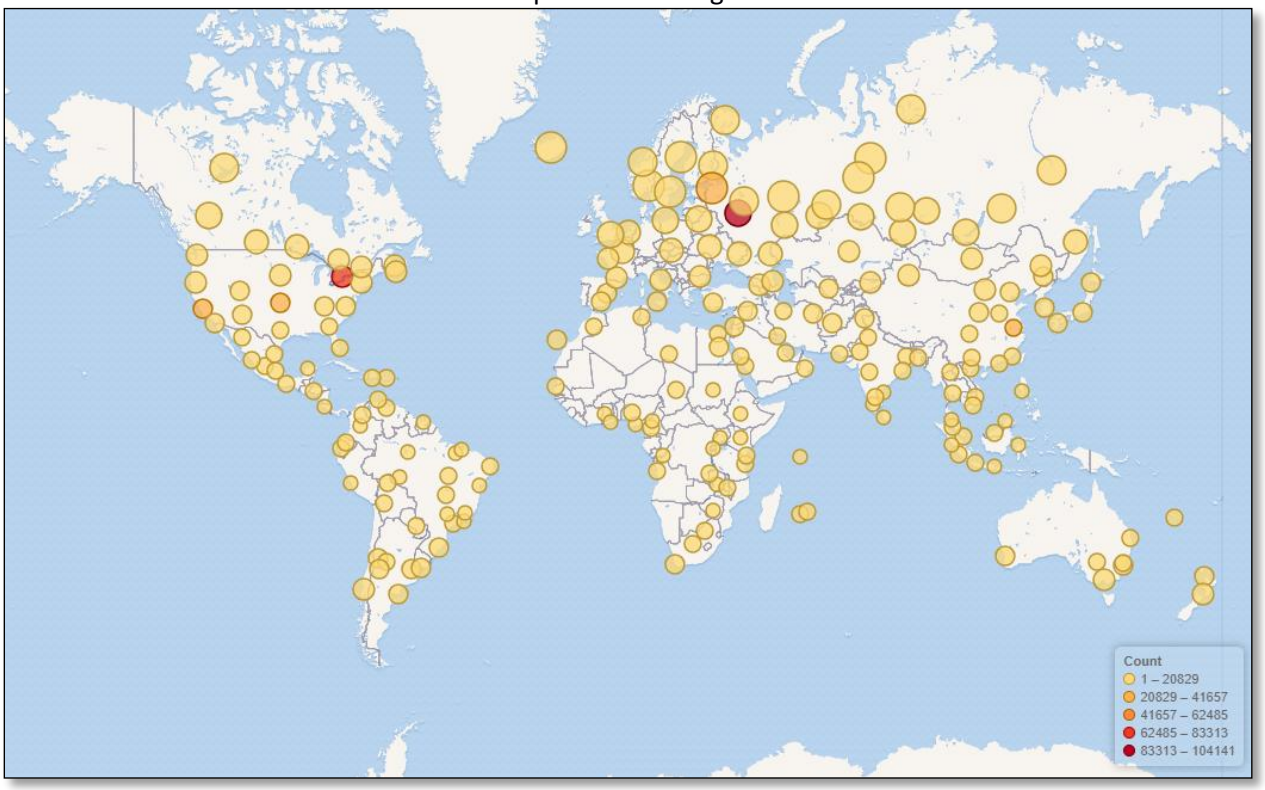

Figure 4: The approximate locations of the attacker's IP addresses

Based on T-POT, 51.65% of attacks are from known attackers, while only 47.18% are from addresses with a bad reputation (figure5).

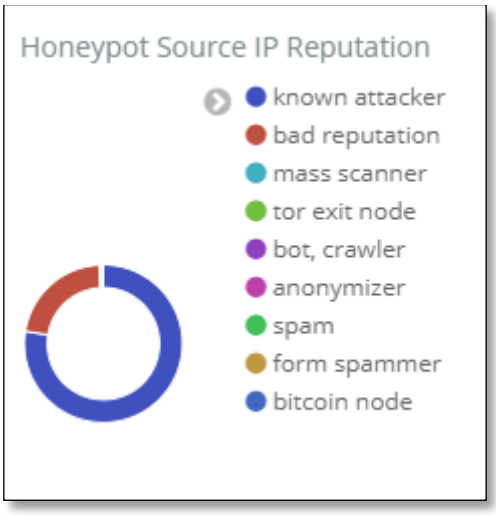

Figure 5: External Honeypot source IP Reputation

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

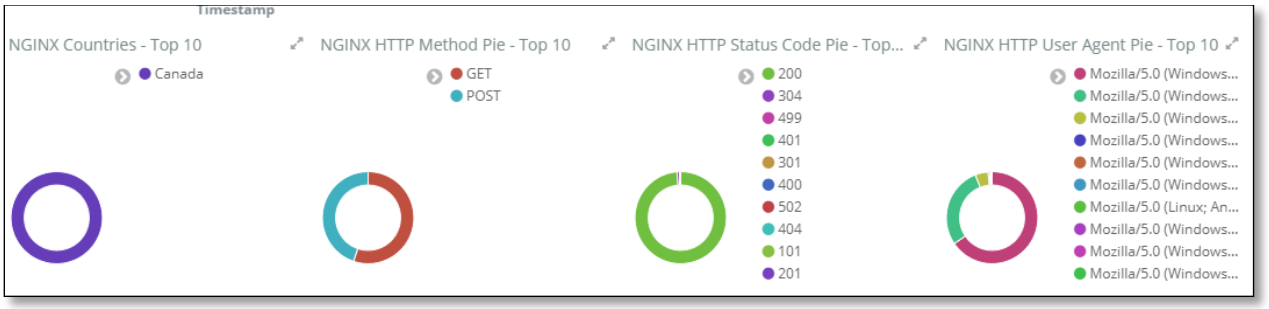

Figure 6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4. Around 18,772 of them are from Master-Integration Ltd.

Table 4: Top 10 Source IP of VNC attack

Username	Number of occurrences
195.201.172.228	34383
109.248.46.113	32347
109.248.46.79	32135
109.248.46.71	32133
109.248.46.99	32128
109.248.46.12	31748
167.99.207.50	25105

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	133305
admin	59018
[blank]	14802
enable	8624
shell	8573
user	5487
guest	5148
Administrator	3665
support	3103
default	2896

Table 6: common password used by attackers

password	Number of occurrences
[blank]	31583
admin	9160
system	8693
1234	8232
sh	7759
123456	7058
password	6510
12345	5954
7ujMko0admin	4622
user	3977

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	518
2	free -m	516
3	ps -x	516
4	export HISTFILE=/dev/null	258
5	export HISTFILESIZE=0	258
6	export HISTSIZE=0	258
7	history -n	258
8	uname	258

Table 8: common command used by attackers grabbed by Mailoney

	command	Number of occurrences
1	QUIT	11903
2	DATA	8183
3	MAIL FROM:<info@ironcladservers.ca>	8182
4	EHLO sie-werden-umgeleitet.com	8181
5	AUTH LOGIN	3680
6	HELO mailserver	3606
7	HELO *.*	95
8	EHLO User	54
9	quit	11
10	STARTTLS	10

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.

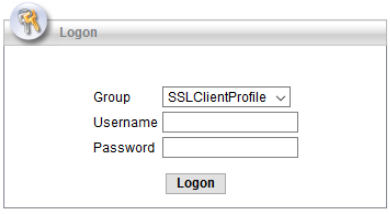

Figure7: Cisco ASA honeypot (First Page)

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.

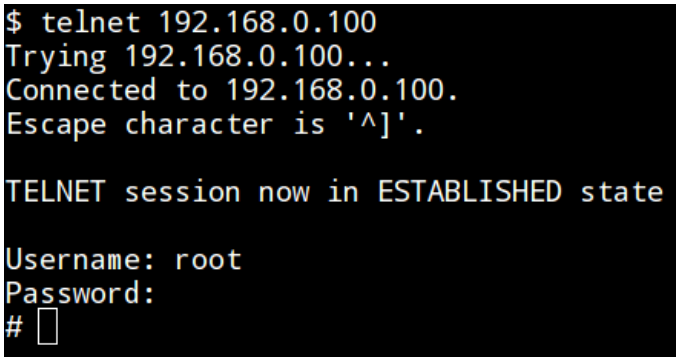

Figure 8: attacks on NGINX

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.

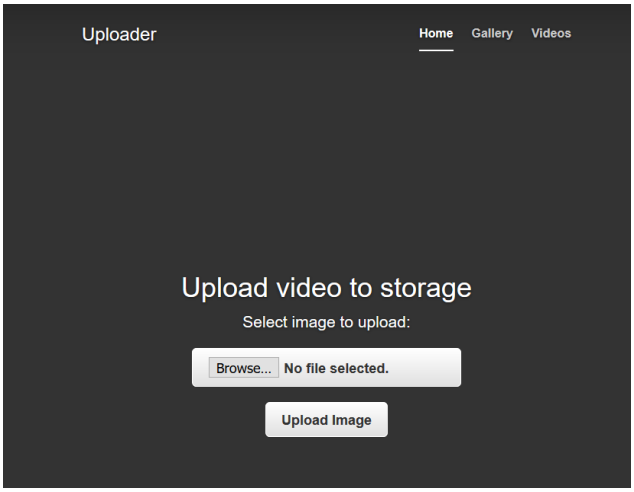

Figure 9 -StrutsHoneypot first page

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, which are demonstrated in Figure 7. We can prove it in Squert and SGUIL which are Security Onion tools to exactly detect attackers (figure 11, 12, 13, 14). 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 from section 3.

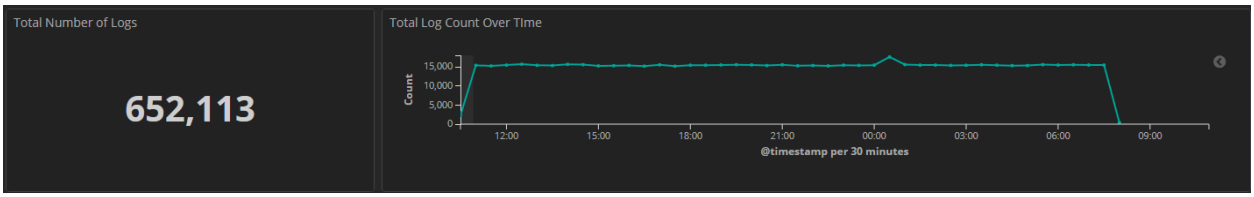

Figure 11: Traffic requested by users

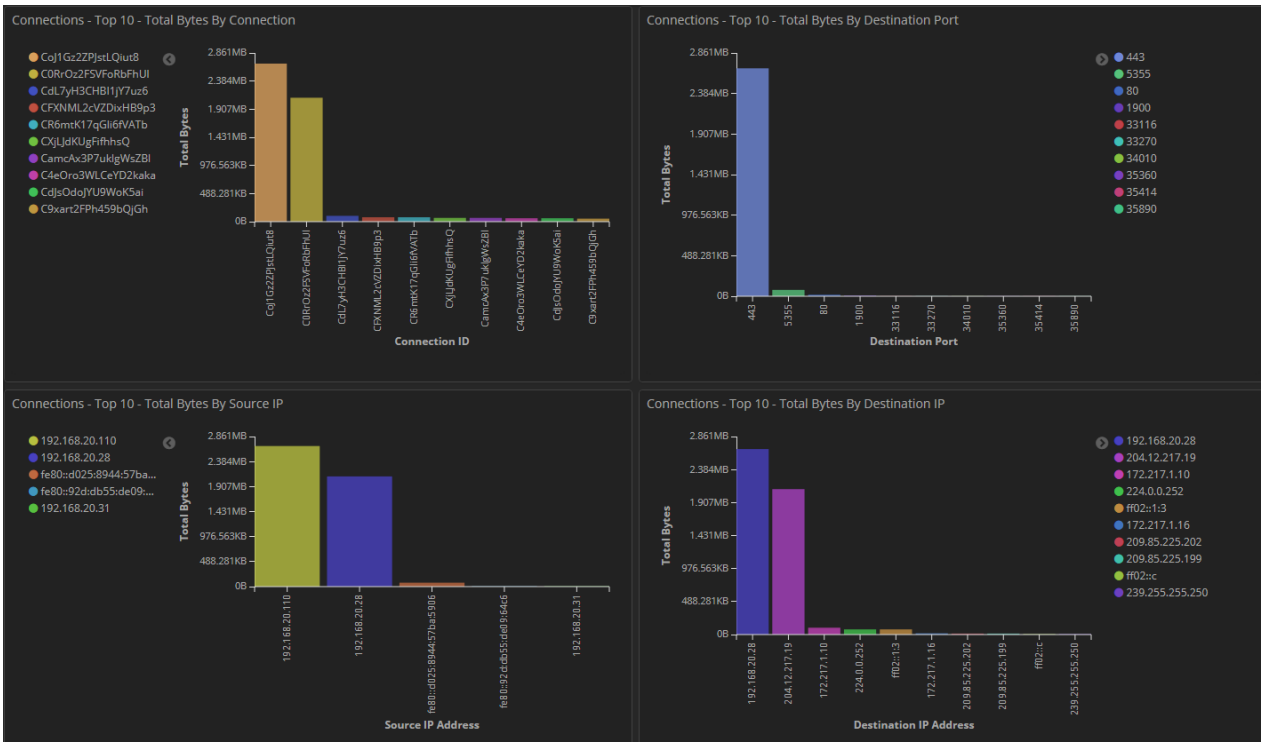

Figure 12: users' traffic inside network

As mentioned, of the activity captured we can see that 44.23% are SSH Scans, 2.89% are MySQL, are 4.77% VNC interactions.

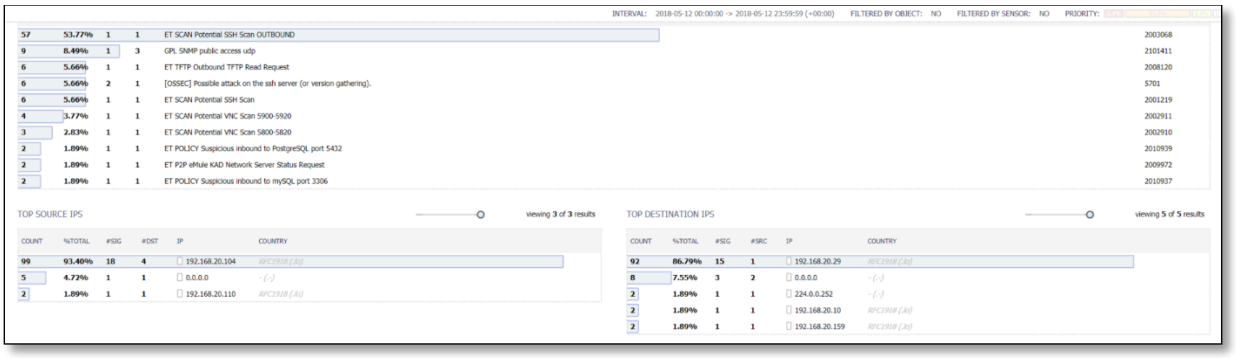

Figure13: Squert summary for attacks

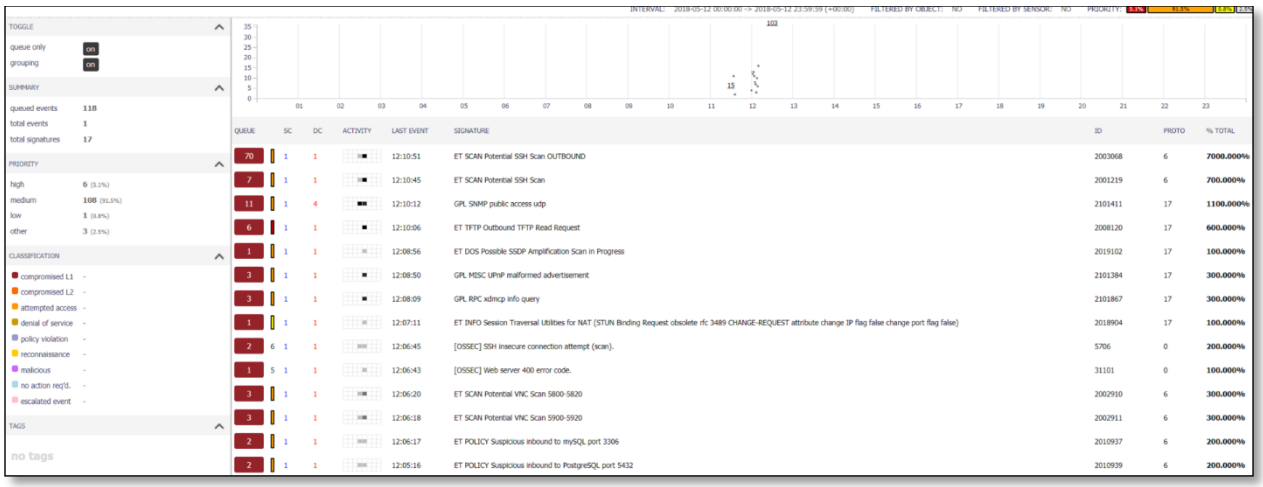

Figure14: Squert shows different attacks on Saturday, 8th of June

4.1 Attacker activities' screenshot- Active Track

Figures 15-19 shows a real attacker screenshot which is installing some software such are BOT attacking social networking, NL Brute to attack other machines.

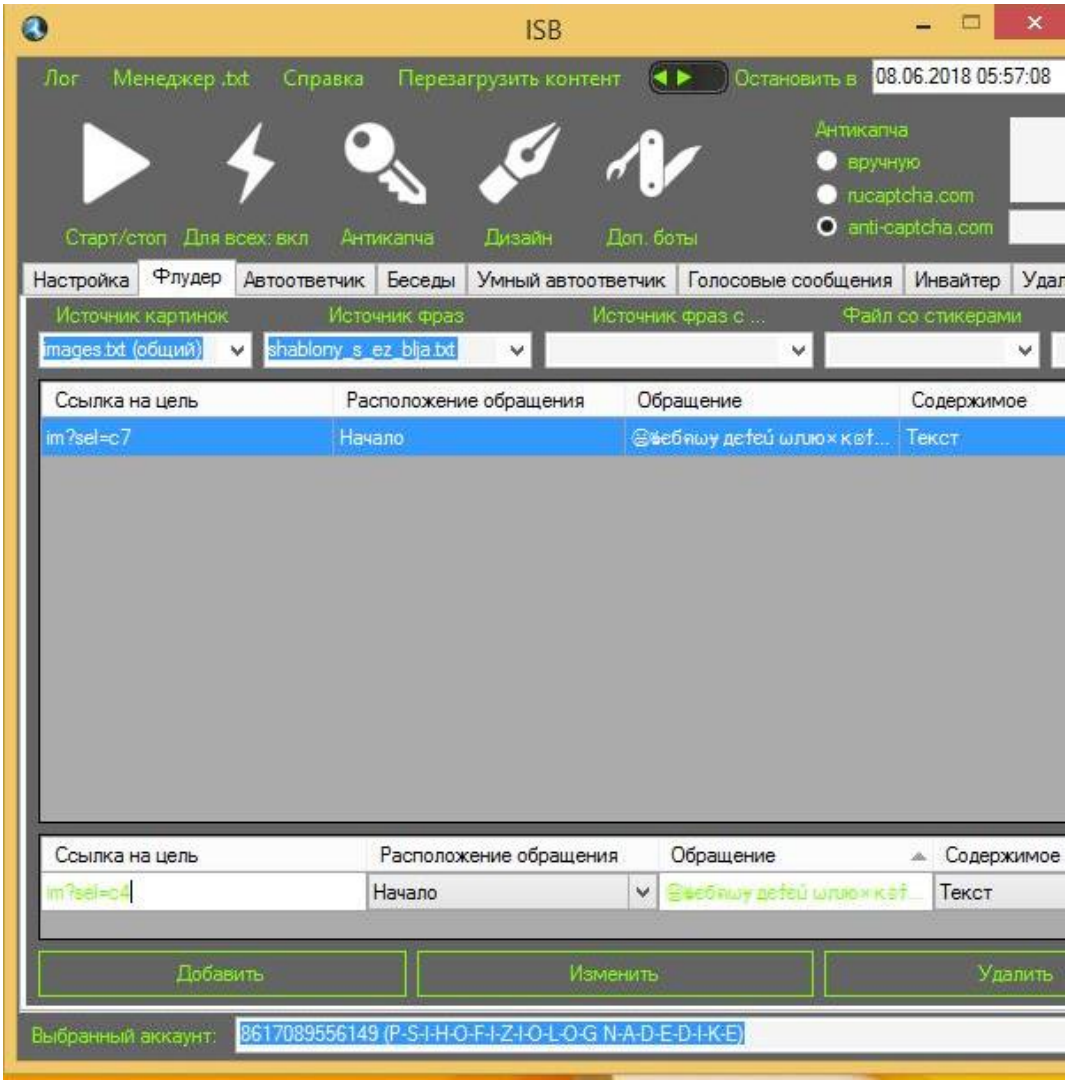

Figure15: ISB for attacking social software vk.com

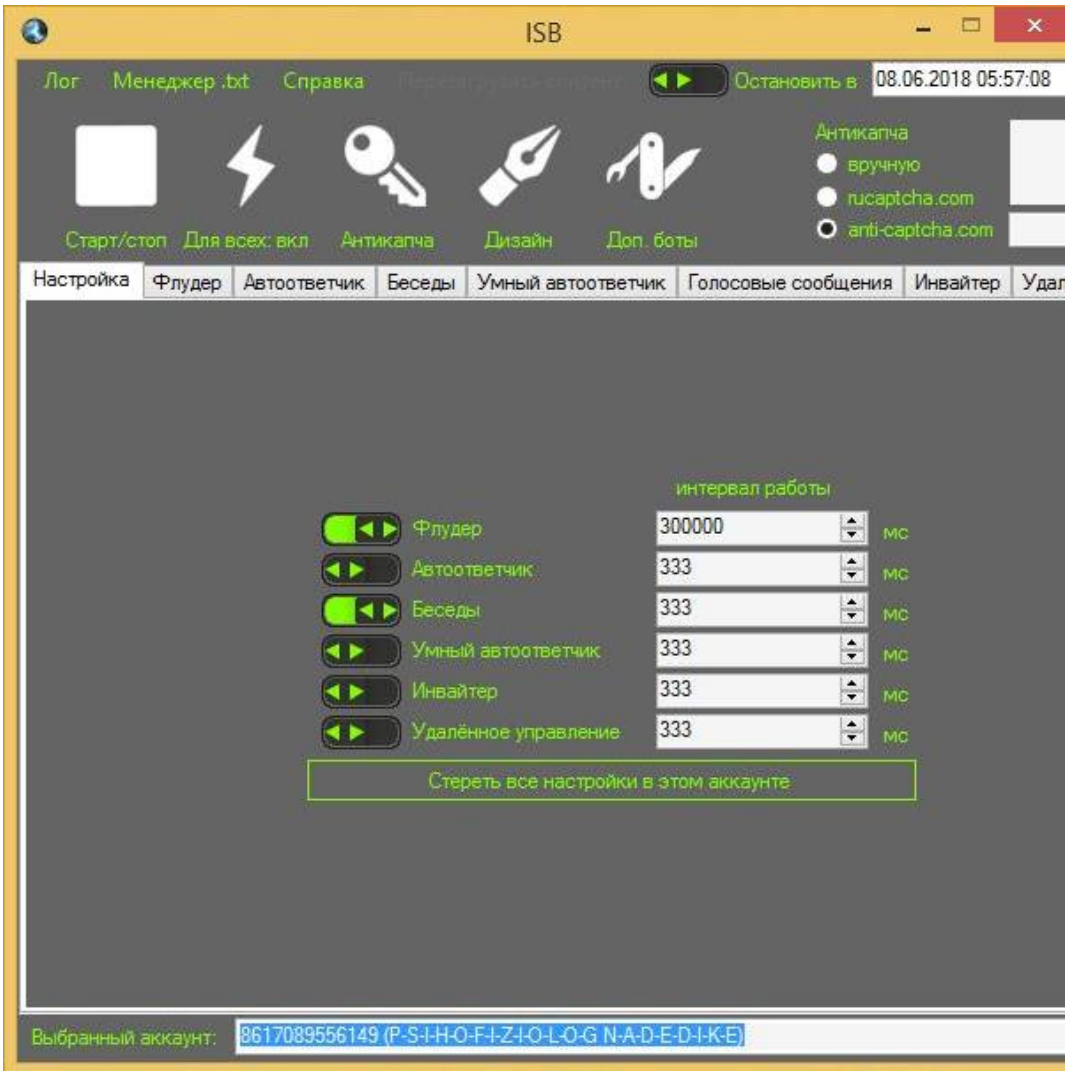

Figure16: defining some parameters

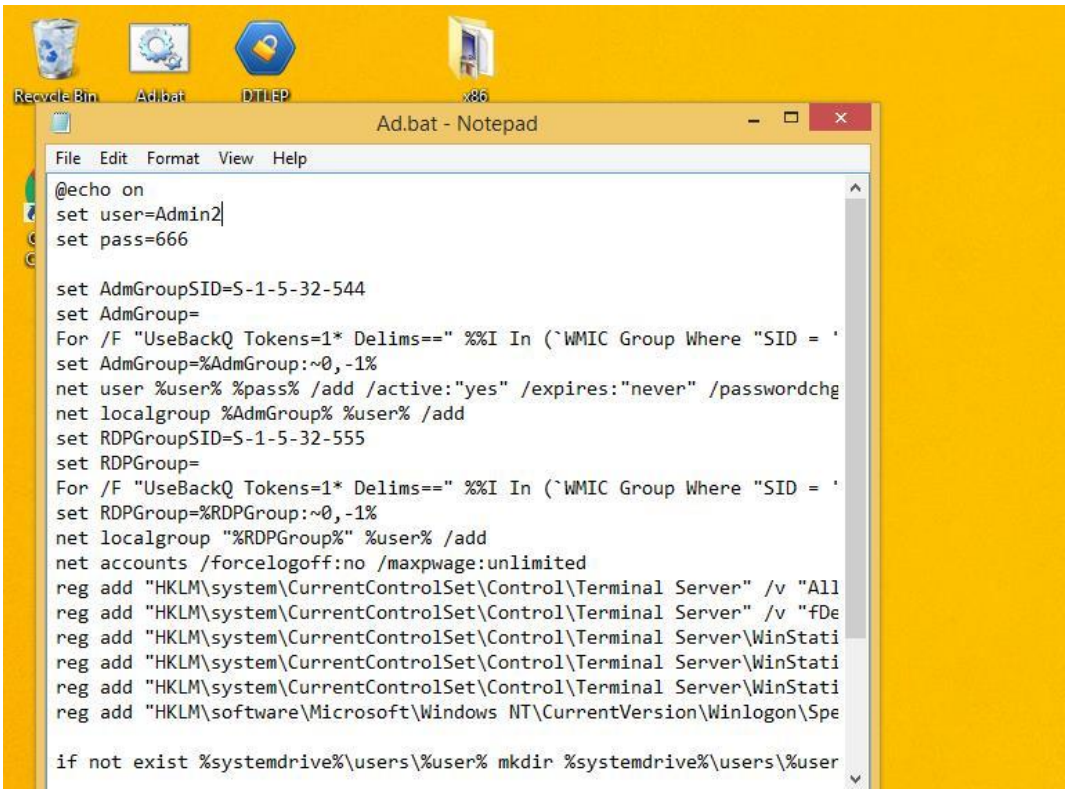

Figure17: Running bash script

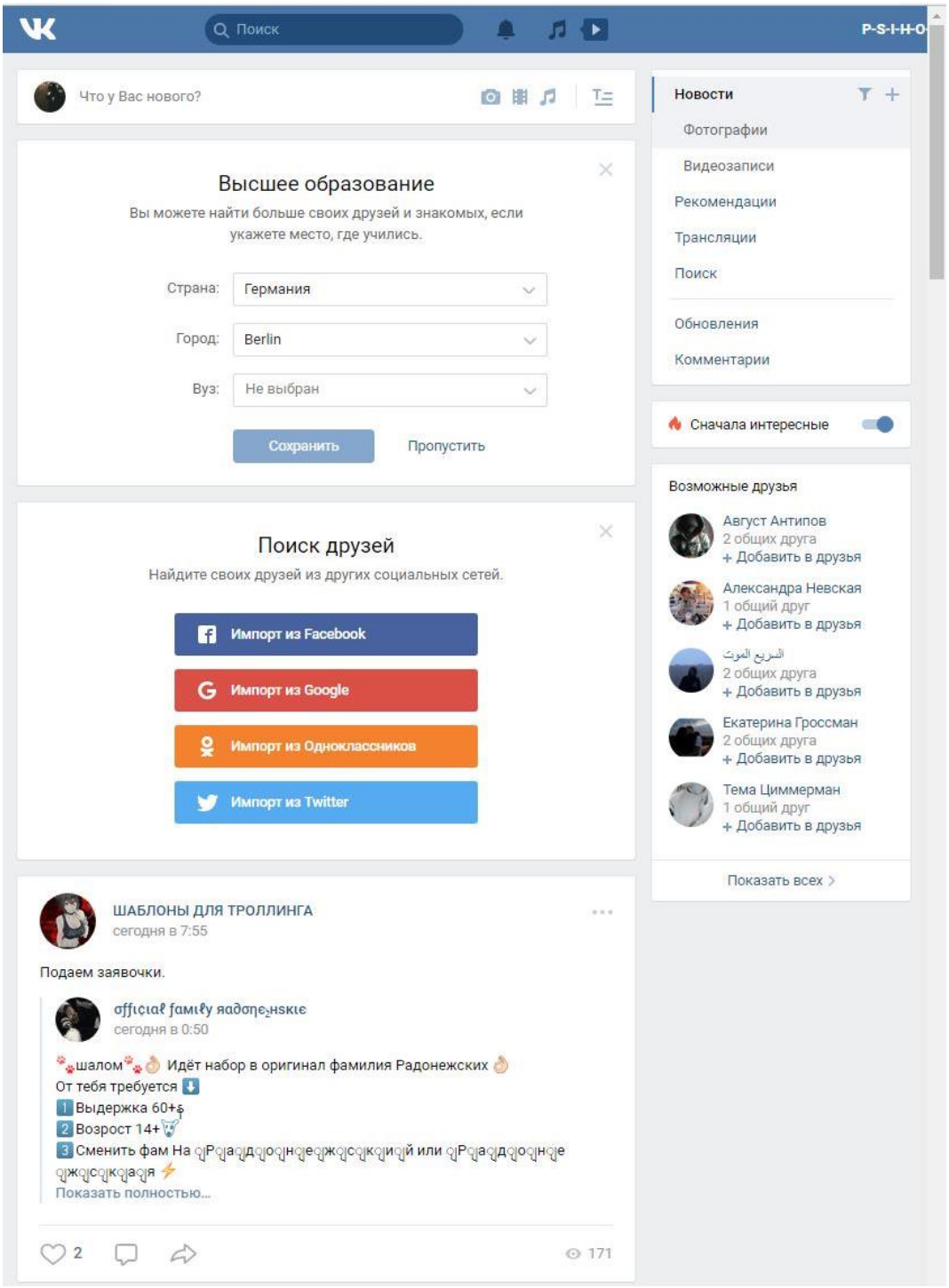

Figure18: Making profile in vk.com

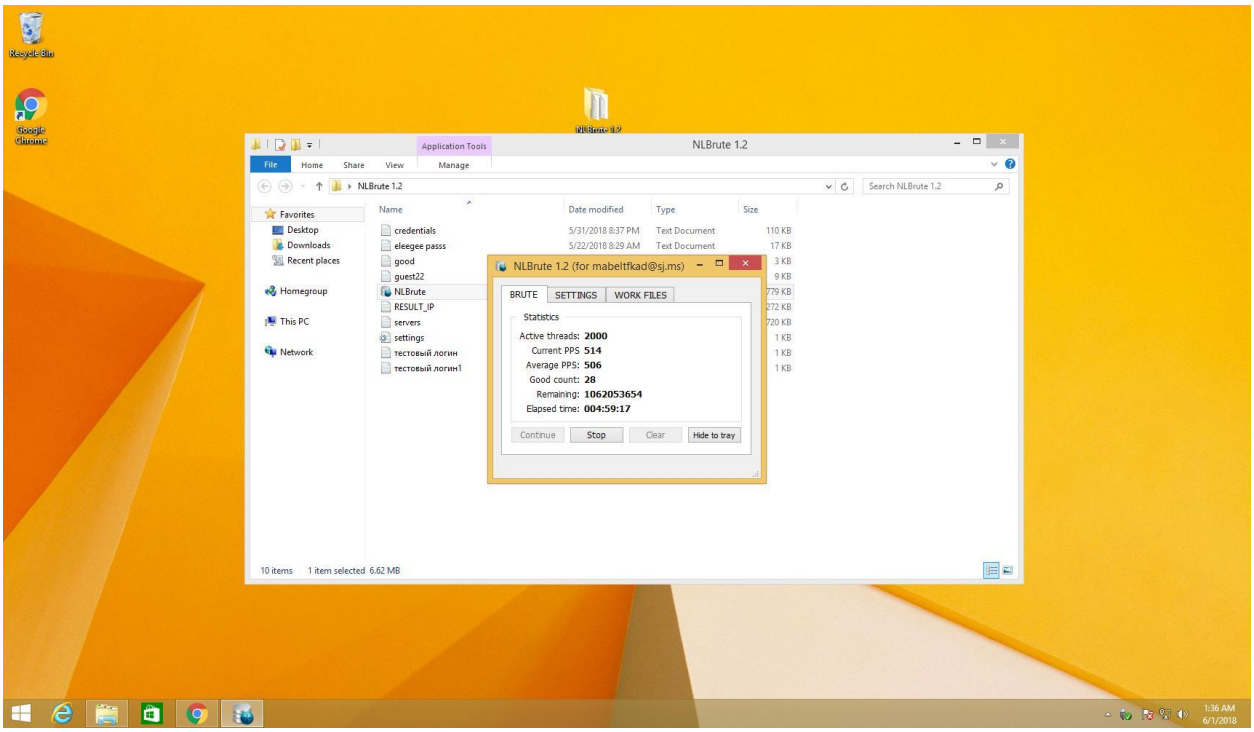

Figure19: Getting result from NLBrute

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 in more effort into removing false noise and analysing data correctly. Figure 20 shows our different diagram in CIC TH.

Furthermore, we have attached all logs to kind of real time system to know who is attacking us. Figure 20 shows this feature.

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 21 demonstrates this feature.

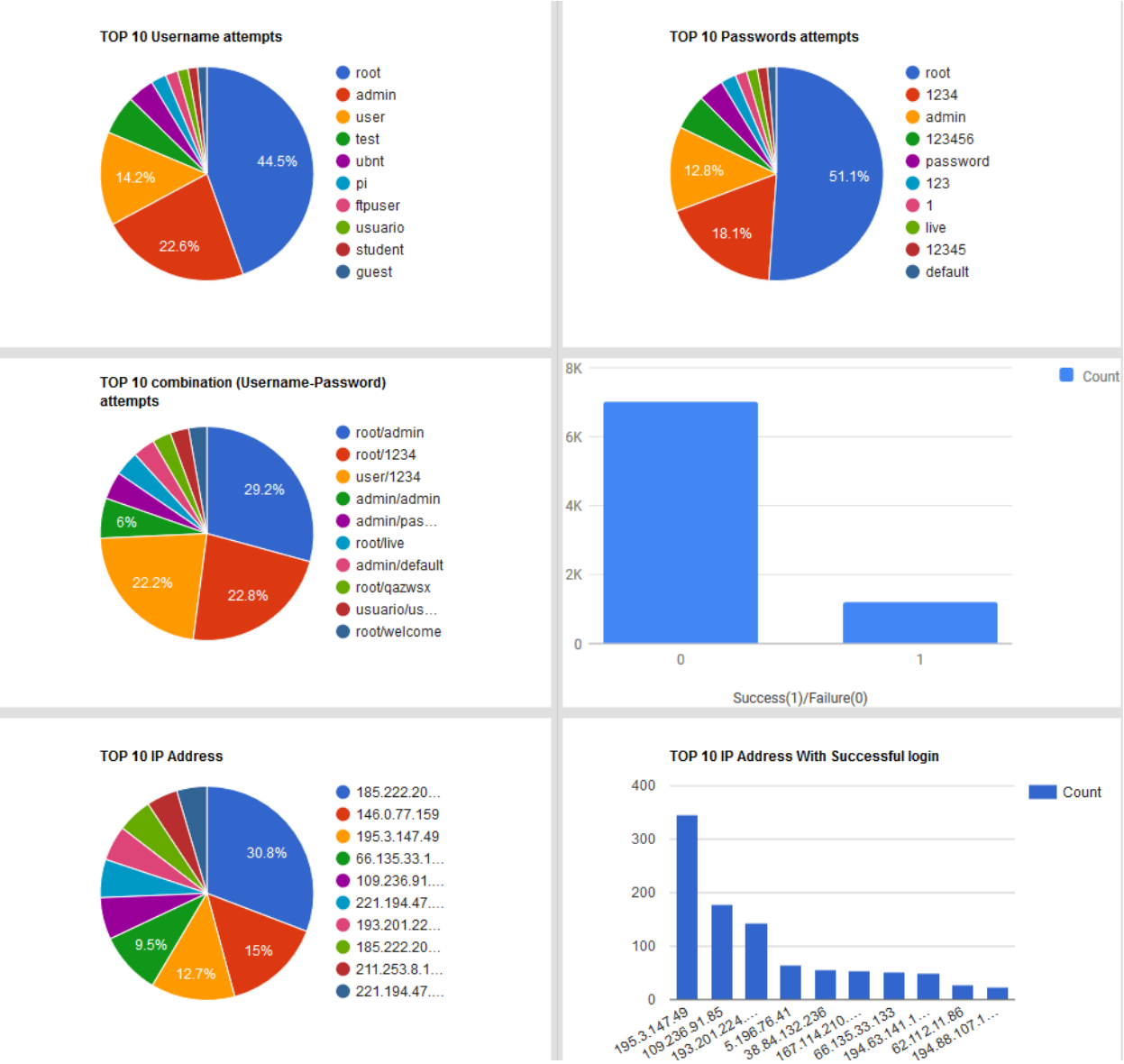

Figure20: UI in CIC Threat Hunting

Playing session: **e3f7a607d046**

```
 /root/systma &gt; /dev/null 2&gt;&amp;1 &amp;
19% [=======>                              ] 547,520      6K/s  eta 5m 38schmod
 0777 systma
20% [=======>                              ] 551,876      6K/s  eta 5m 46schmod
 u+x systma
21% [========>                             ] 595,683      6K/s  eta 5m 32s./sys
tma &
23% [========>                             ] 639,483      6K/s  eta 5m 16schmod
 u+x dos6cc4
27% [==========>                           ] 754,823      7K/s  eta 4m 23s./sys
tma &
28% [==========>                           ] 794,243      7K/s  eta 4m 16scd /t
mp
31% [============>                         ] 867,243      8K/s  eta 3m 54secho
"cd  /root/">>/etc/rc.local
34% [=============>                        ] 950,463      8K/s  eta 3m 31secho
"./sysem&">>/etc/rc.local
36% [==============>                       ] 994,263      8K/s  eta 3m 24secho
"./systma&">>/etc/rc.local
37% [==============>                       ] 1,033,659    8K/s  eta 3m 18secho
"/etc/init.d/iptables stop">>/etc/rc.local
42% [================>                     ] 1,158,885    8K/s  eta 2m 59s

*** End of log! ***
```

Figure21: CIC TH Playback