Honeynet Weekly Report
Canadian Institute for Cybersecurity (CIC)

Report Capture: 16-01-2018 to 23-01-2018

1-Introduction

The first honeypot studies released by Clifford Stoll in 1990, and from April 2008 the Canadian Honeynet chapter was founded at 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 on the tables for Hackers and computer security experts and it consists of a computer, data or a network site that appears to be part of a network but which is isolated, and which seems to contain information or a resource that would be of value to attackers.

There are some benefits of having 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 behaviour of attackers, investigate tactics and practices of hacker community and share learned lessons with IT community and appropriate forums in academia and law enforcement in Canada. So, CIC decided to use cutting edge technology to collect dataset for honeypot.

These reports are generating 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 Honeynet dataset, we have defined a separated network with these services:

- Email Server(SMTP-IMAP)
- FTP Server
- File Server
- Web Server
- SSH
- Http
- Https

Each user has a real behaviour and surf the Internet based on above protocols. Web server is accessible for public and anyone who can see the website. Inside network, we put an **Untangle** firewall at the edge

of network and NAT different services for public user. Traffic of network passes through firewall based on users surfing via network. Some ports such as 20, 21, 22, 53, 80, 143, 443 are open on the firewall based on services are defined on the network.

To absorb attackers, beside real network, some ports and services intentionally have been opened. Some policies such as password have not been regarded.

Real data traffic is passes through PCs which are separated and not accessible in network and via Tap all traffic is captured by TCPDUMP.

3- Logging & Data Collection

Everything that happens on the honeypot is logged for analysis. These are some features of logs:

- Source IP
- Source Port
- Destination
- Destination Port
- Protocol
- Timestamp
- Flow Duration
- Flow Bytes
- Fwd Packets
- …

As above-mentioned **CICFlowMeter** offers more flexibility in terms of choosing the features you want to calculate, adding new ones, and also having a better control of the duration of the flow timeout.

The traffic which is captured by TCPDUMP is analysed with **CICFlowMeter** which is generated by CIC. We analysis flow of traffic to know whom, when and which server is attacked by attackers

Also, we use Security Onion for analysing inside traffic and **Untangle** firewall for traffic of edge of network. The traffic of inside and outside firewall is captured by two taps and again it is analysed by **CICFlowMeter**.

To simulate SSH for attackers, we use Kippo tools and is intended to mimic a SSH command. Kippo can capture commands and the password users enter. Some easy password such as 1234, 123,… are entered in Kippo database so attackers can easily reach the server.

4- Analysis and Result

4.1 login attempts

We analyzed the IP addresses that made login attempts using the Domain Bulk look IP , We received login attempts from 101 unique IP addresses in 26 countries; the breakdown by country is shown in table 1.

Table1: IP breakdown by country

IP	Country	Number of Attack
222.186.30.99	China	498
103.99.2.4	Vietnam	120
62.112.11.134	Netherlands	58
217.23.1.87	Netherlands	57
62.112.11.7	Netherlands	42
62.112.11.94	Netherlands	38
5.188.10.156	Croatia	30
182.100.67.201	China	30
194.88.107.165	Netherlands	29
62.112.11.223	Netherlands	26
121.18.238.39	China	22
194.88.107.163	Netherlands	22
195.3.147.47	Latvia	21
121.18.238.125	China	16
193.201.224.206	Ukraine	16
221.194.47.221	China	16
194.88.107.164	Netherlands	16
221.194.47.233	China	16
45.32.67.137	United States	16

This list is proved by our **Security Onion**, which is demonstrated in Figure1.

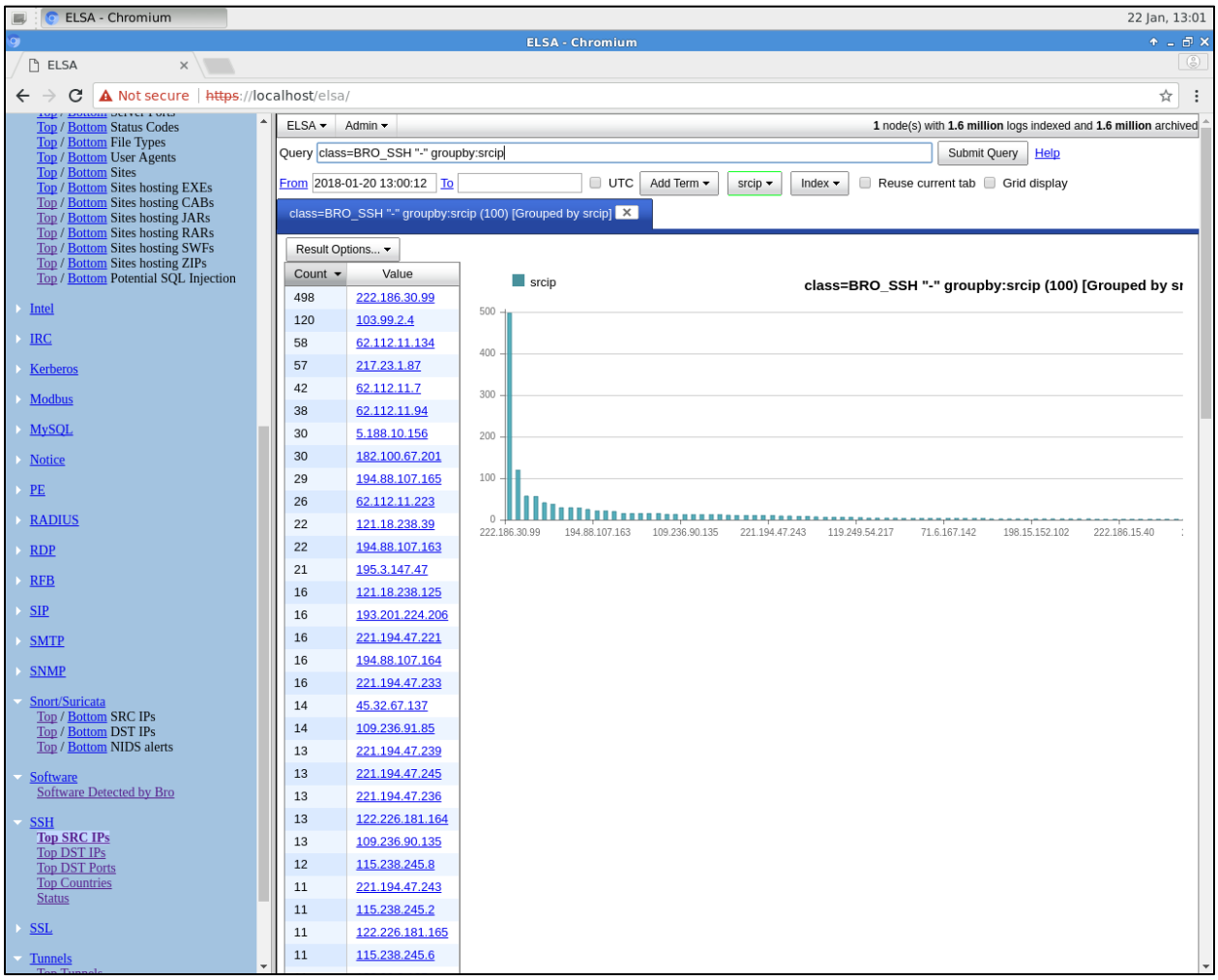

Figure1: attack Count

Based on IP and with using GEO location tools, we can demonstrate approximate locations of IP address which is presented on Figure 2.

Figure2: The approximate locations of the IP addresses

Based on firewall report, from 901 sessions, around 90% of sessions is on SSH, 3% on FTP, 5% on HTTP and finally 2% is on POP3 (Figure 3).

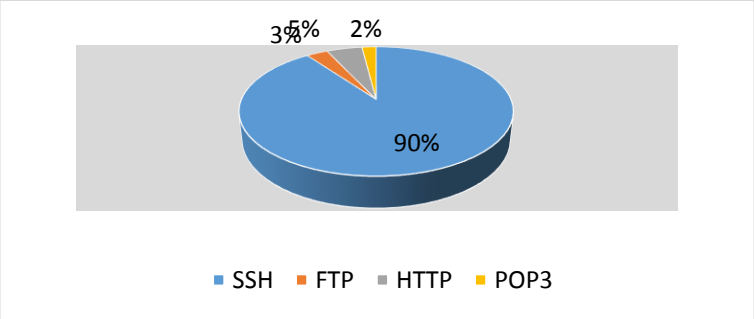

Figure3: top sessions ports

4.2 TOP Username and password for brute force attack

For brute force attack, attackers use kind of username and password which is listed in table 2,3:

Table2: common username used by attackers

	username	Number of occurrence
1	root	3461
2	admin	873
3	user	743
4	pi	106

Table3: common password used by attackers

	password	Number of occurrence
1	123	1535
2	1234	1155
3	123456	146
4	password	110

Security tips: It is recommended for preventing brute force attack, use username which is not common such as user457 or CompanyNameFamilyName. Using common username opens up opportunity for attackers to brute force your server. For example using username such as root, admin, user, usr are bad practise of using username.

4.3 TOP Commands

Table 4, shows the most common commands used by attackers. (All commands are available in captured data)

Table4: common command used by attackers

	command	Number of occurrence
1	ls	5
2	df -h	4
3	rm -f	2
4	Running their own code	1

We are dealing with kind of Bot which use kind of code for changing file system. (All executed commands by Bots through SSH are available in captured data)

4.4 Hours of login

Based on this week observation attackers try to attack 24 hours. It seems that kind of Bot is responsible of attacks, so attackers run it 24 hours to find a gap in any servers.

4.5 Inside Network

Inside Network activities which are logged by **Security Onion** are shown in figures 4, 5 and 6. This traffic includes http, ftp, SSH, and system logs.

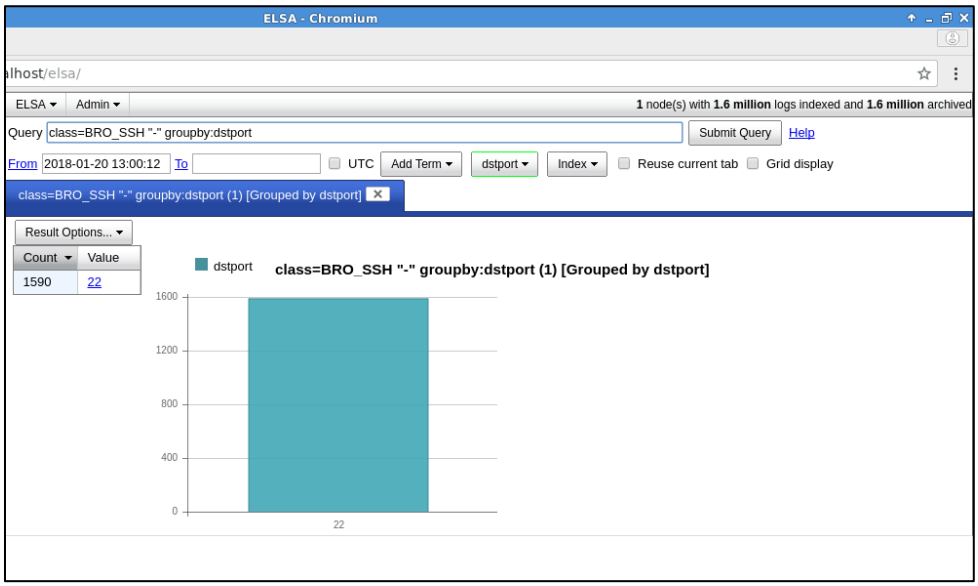

Figure4: TOP PORT

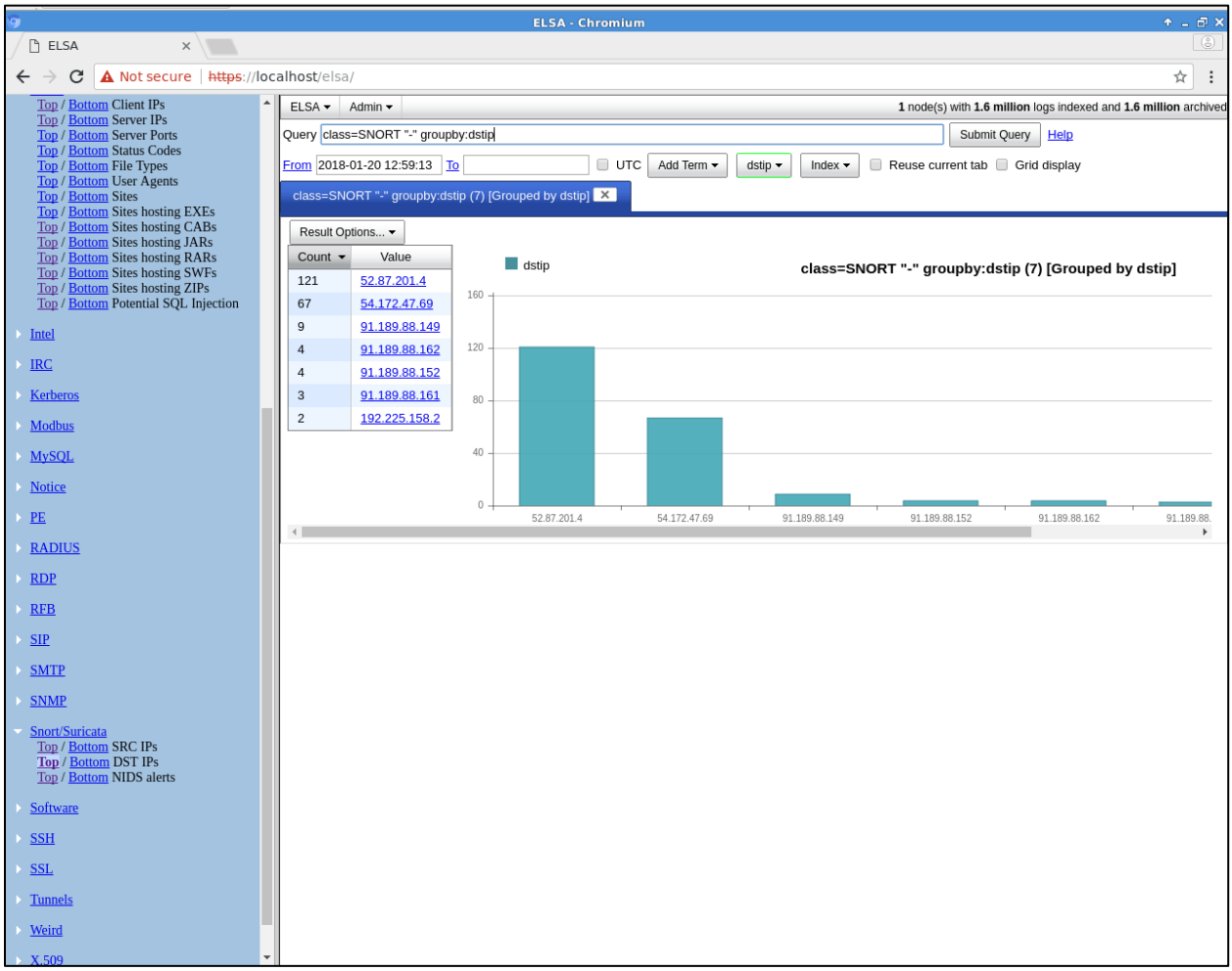

Figure5: TOP Destination IP from Local Users

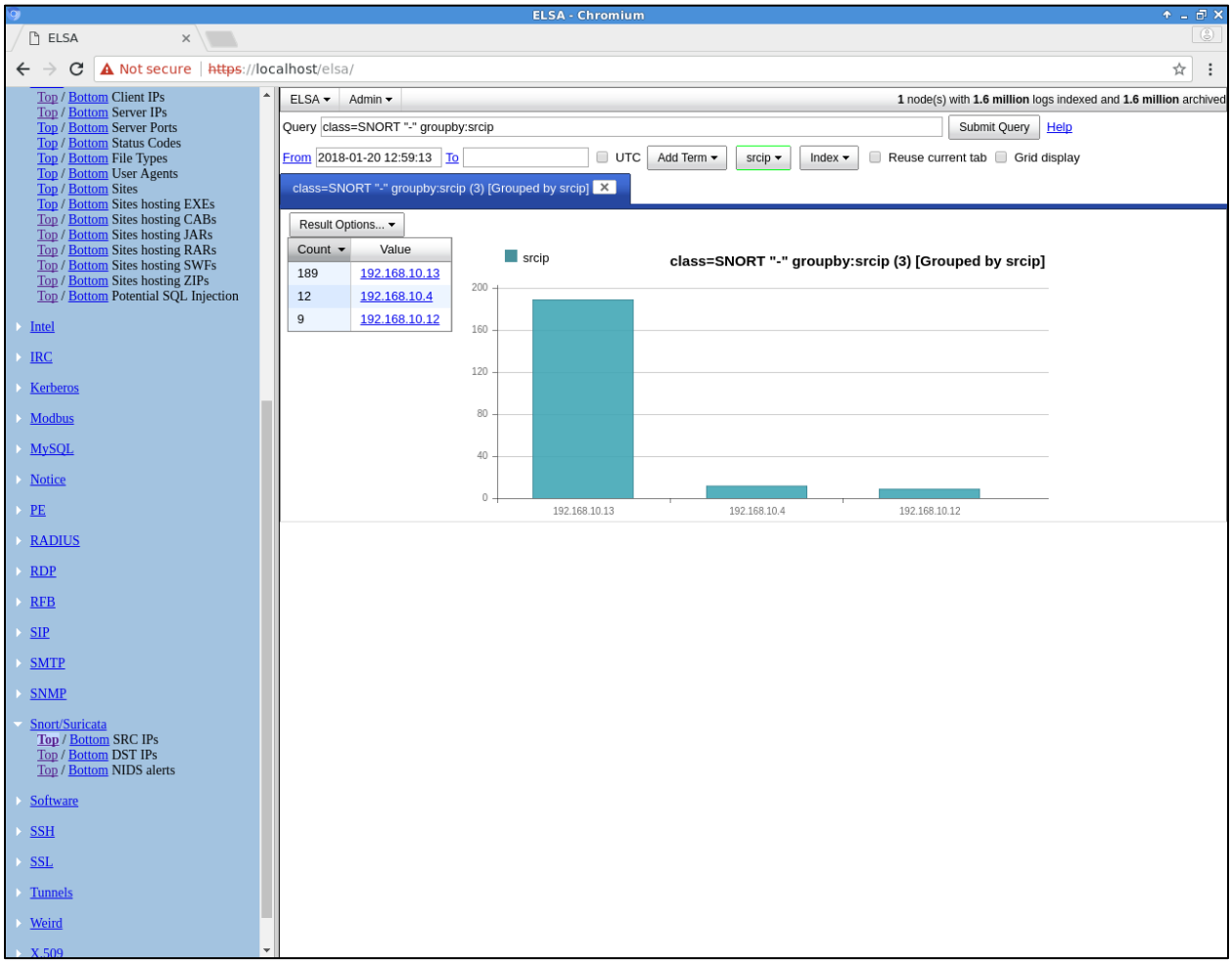

Figure6: TOP Local Users