Report Capture(2): 24-01-2018 to 31-01-2018

1-Introduction

The first honeypot studies released by Clifford Stoll in 1990, and from April 2008 the Canadian Honeynet chapter was founded at 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 Honeynet dataset, we have defined a separated network with these services:

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

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 network, we put **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. 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 real generated data on PCs is mirrored through TAPs for capturing and monitoring 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 previously mentioned **CICFlowMeter** offers more flexibility by: including more features, giving you the ability to easily add new ones, and also giving you better control over the duration of the flow timeout.

The traffic which is captured by TCPDUMP is analysed with **CICFlowMeter** which is generated by CIC. We analyse the 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 on the edge of the network. The traffic inside and outside the firewall is captured by two TAPs and again it is analysed by **CICFlowMeter**.

We use **Kippo tools** to simulate SSH for attackers, 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 25 countries; the breakdown by country is shown in table 1.

Table1: IP breakdown by country

IP	Country	Number of Attack
182.100.67.201	China	922
103.99.2.4	Vietnam	300
195.3.147.49	Latvia	153
202.153.220.62	Australia	92
193.201.224.206	Ukraine	92
58.214.22.74	China	92
109.236.91.85	Netherlands	86
5.188.10.156	Croatia	78
221.194.47.239	China	56
221.194.47.221	China	55
121.18.238.39	China	53
221.194.47.243	China	48
221.194.47.245	China	47
115.238.245.8	China	46
221.194.44.211	China	45
221.194.47.221	China	45
221.194.47.233	China	44
221.194.47.236	China	42
180.250.19.91	Indonesia	41

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

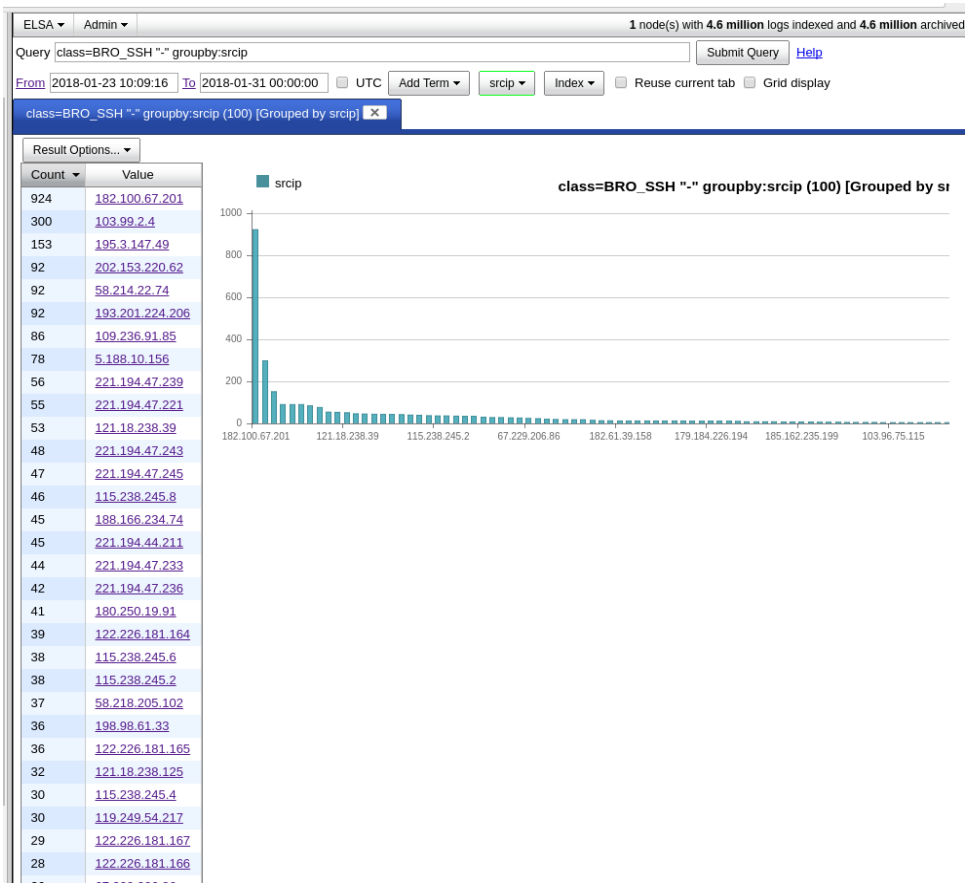

Figure1: attack Count

Based on IP and 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 1000 sessions, around 92% of sessions are on SSH, 2% are on FTP, 4% are on HTTP and 2% are on POP3 (Figure 3).

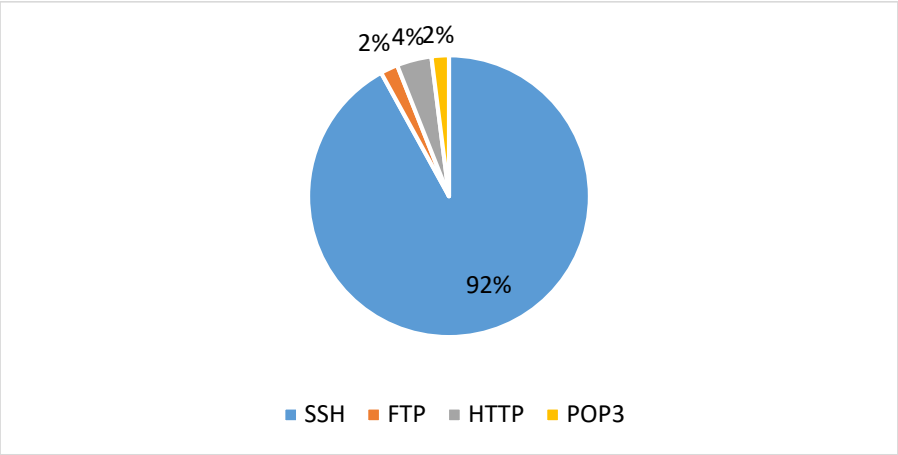

Figure3: top sessions ports

4.2 TOP Username and password for brute force attack

For brute force attack, attackers used usernames and passwords which are listed in tables 2 and 3:

Table2: common username used by attackers

	username	Number of occurrence
1	root	5604
2	admin	1900
3	user	823
4	pi	187
5	support	108

Table3: common password used by attackers

	password	Number of occurrence
1	123	2747
2	1234	1699
3	123456	306
4	password	220

Security tips: It is recommended that to preventing brute force attacks, you should use usernames which are not common such as user457 or CompanyNameFamilyName. Using common usernames creates opportunity for attackers to brute force your server. For example using username such as root, admin, user, usr are bad practise and are extremely vulnerable.

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	Running their own code	10
2	mount	5
3	rm -f	4
4	ls	3

We are dealing with a kind of Bot which uses the above commands to change the 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 24/7. It seems that some kind of Bot is responsible for the attacks. Attackers run it 24/7 to find a gap in any server.

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.

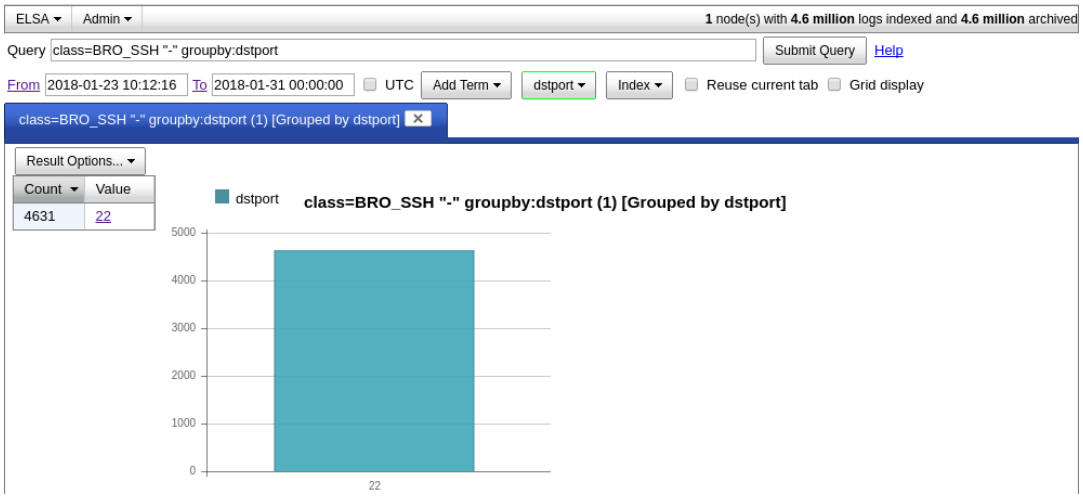

Figure4: TOP PORT

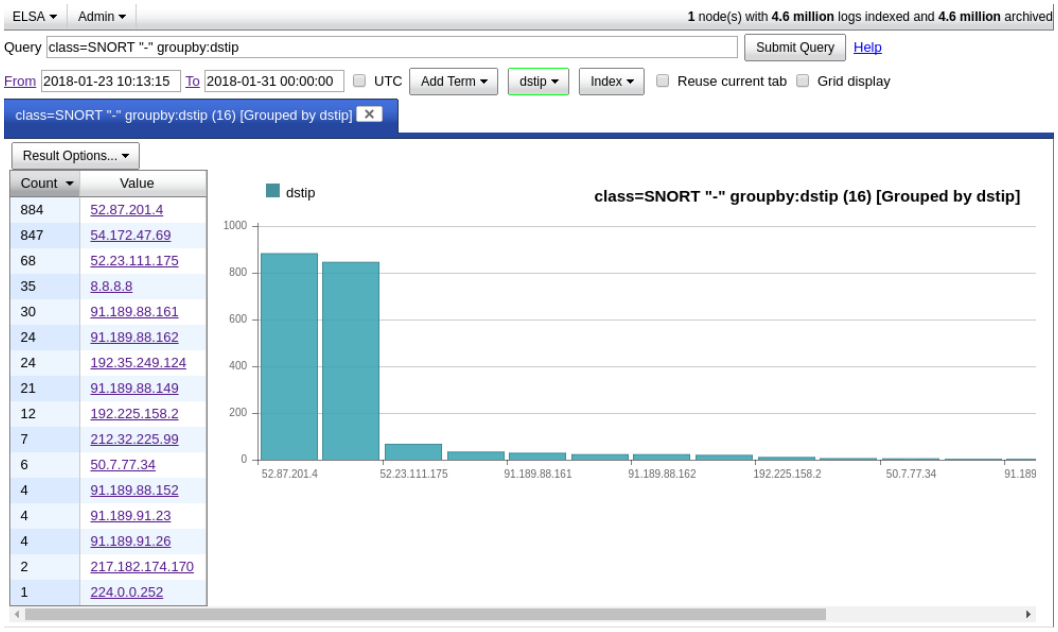

Figure5: TOP Destination IP from Local Users

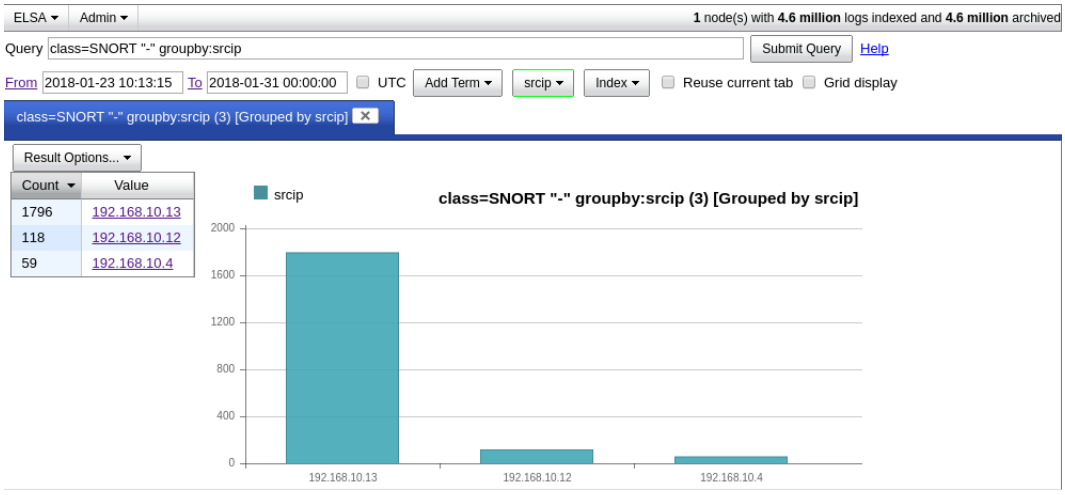

Figure6: TOP Local Users