Honeynet Weekly Report
Canadian Institute for Cybersecurity (CIC)

Report Capture(4): 08-02-2018 to 16-02-2018

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)(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 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.

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 bots want to produce spam we can grab it through "Contact Form 7 Honeypot"(Figure 1).

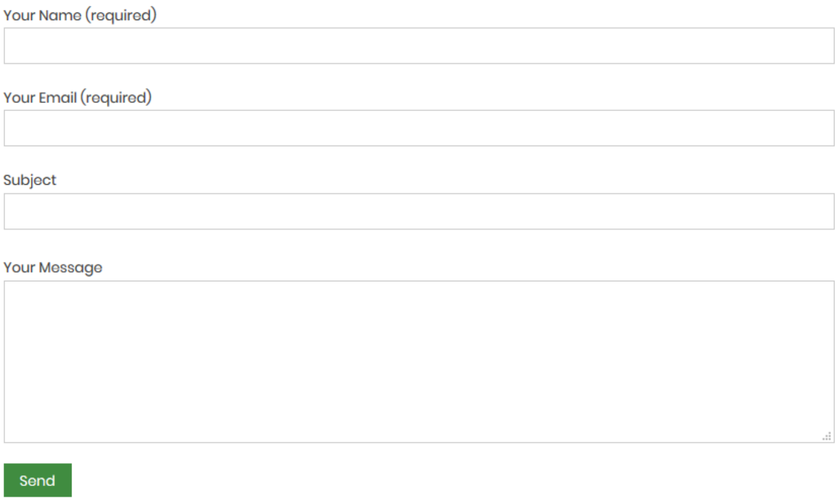


Figure1: Contact Form 7 Honeypot

Also, we use T-POT tool which is equipped with several tools. T-Pot is based on well-established honeypot daemons, 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 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 and our tools. There are two TAPs in the network for capturing network activities.

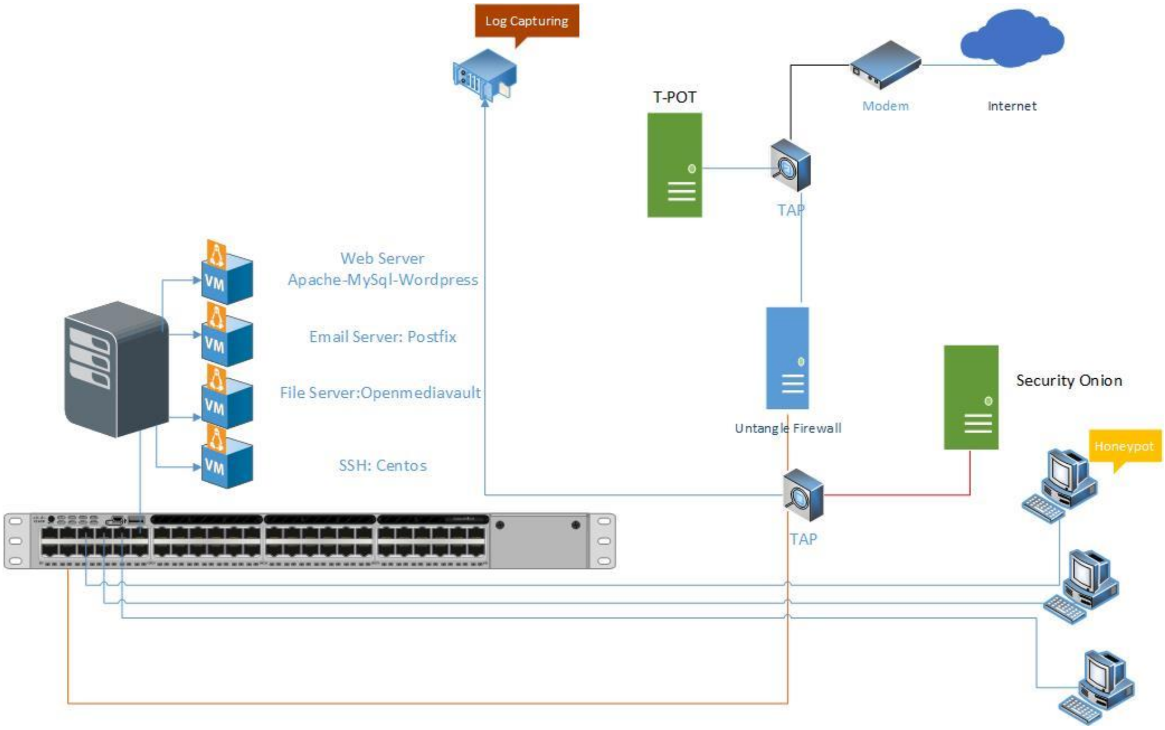


Figure2: Network Diagram

To absorb attackers, some ports and services have been intentionally opened. Best practise policies regarding passwords have been disregarded.

Real data traffic is passing through PCs which are separated and not accessible through the network. All traffic is captured via TAPs and 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 analysis flow of traffic to know who, when and which server is being attacked.

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**.

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

Also, this week's report is based on T-POT and its features. Therefore, some results between outside the firewall and inside the firewall is the same.

4- Analysis and Result

4.1 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	201139
China	18912
Brazil	18399
Netherlands	14432
United States	4272
France	4006
Turkey	3727
Japan	3466
Republic of Korea	2040
Cyprus	2017

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

Table2: Top 10 Source IP

Source IP	Number of Attack
5.188.86.194	12626
61.177.172.137	12624
5.188.86.168	12620
5.188.87.52	11528
5.188.86.208	10909
5.188.86.167	10034
5.188.87.51	9995
109.248.9.105	9307
5.188.86.209	8839
5.188.86.210	8808

In figure3, top 5 of countries are demonstrated by related ports. For example attacks from Russia have been 87.91% through port 2222, 5.92% through port 25, 2.96% through port 443, 1.36% through port 80, and 0.83% through port 587.

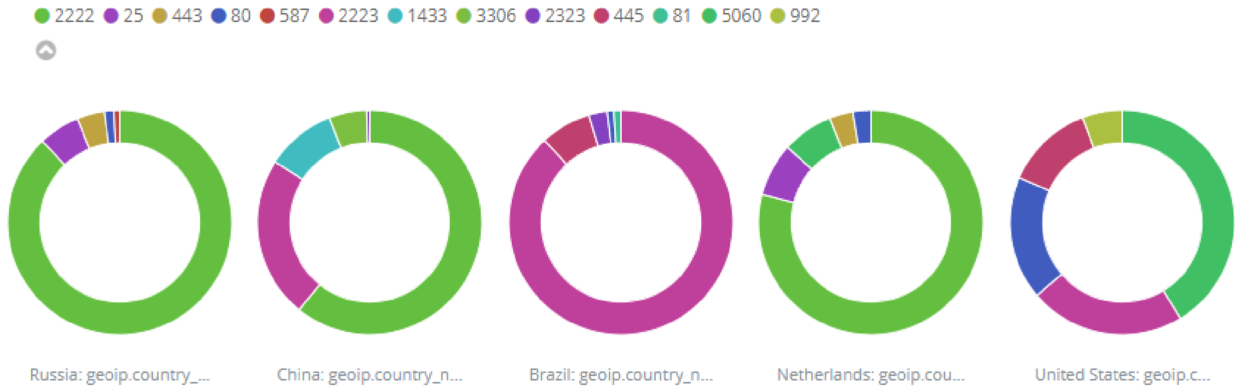


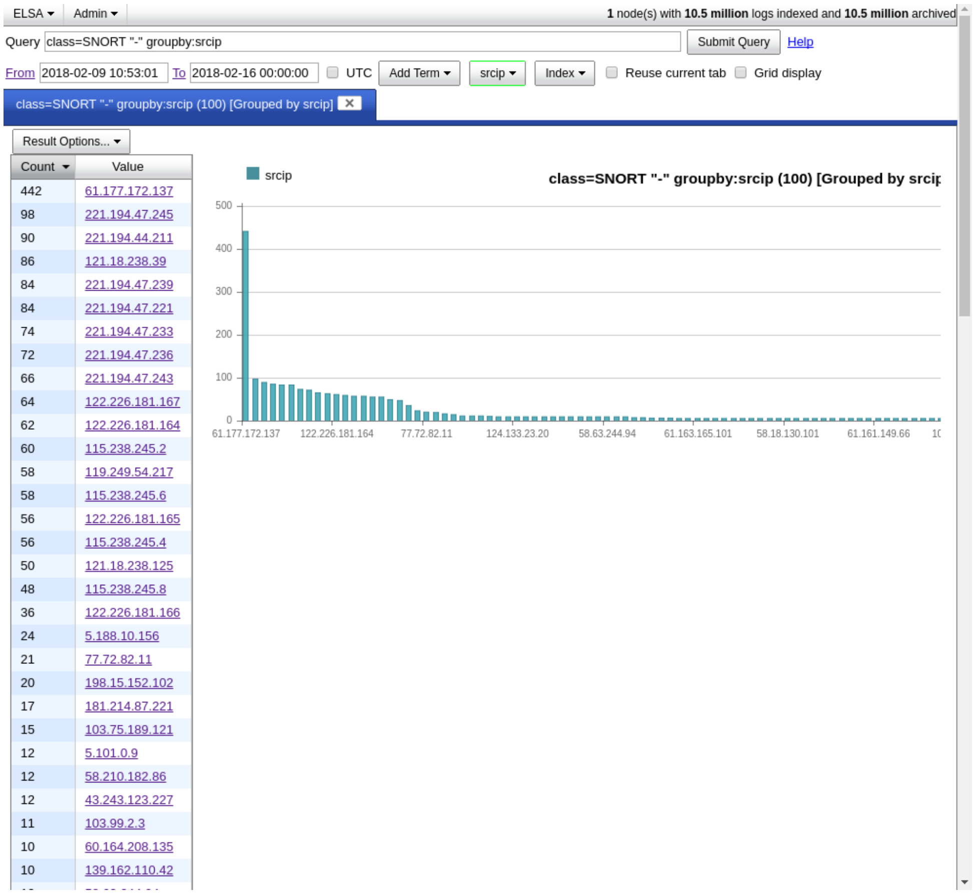
Figure3: Honeypot by country and port

There are two CVE-ID for attacks, CVE-2003-0567 and CVE-2017-0143 which are demonstrated in Table3.

Table3: Top 10 Source IP

CVE-ID	Numbers
CVE-2003-0567	16885
CVE-2017	12

Inside of our network, **Security Onion** is capturing the number of attacks which is demonstrated in Figure4. Also we can prove it in Squert and SGUIL which are tools of Security Onion to exatcly detect attackers(figure 5,6).



1 node(s) with 10.5 million logs indexed and 10.5 million archived

Query class=SNORT "-" groupby:srcip

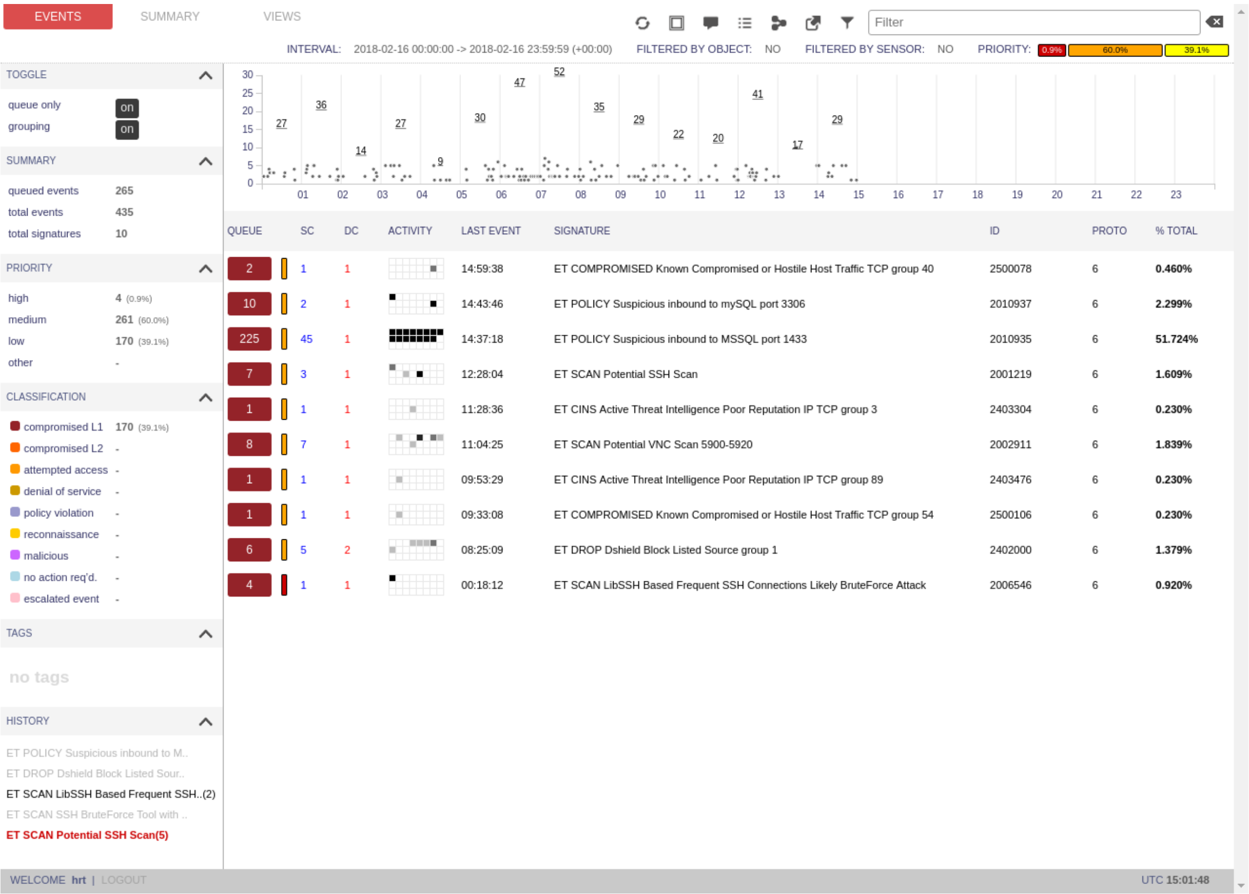
From 2018-02-09 10:53:01 To 2018-02-16 00:00:00 □ UTC □ Reuse current tab □ Grid display

class=SNORT "-" groupby:srcip (100) [Grouped by srcip]

class=SNORT "-" groupby:srcip (100) [Grouped by srcip

Count	Value
442	61.177.172.137
98	221.194.47.245
90	221.194.44.211
86	121.18.238.39
84	221.194.47.239
84	221.194.47.221
74	221.194.47.233
72	221.194.47.236
66	221.194.47.243
64	122.226.181.167
62	122.226.181.164
60	115.238.245.2
58	119.249.54.217
58	115.238.245.6
56	122.226.181.165
56	115.238.245.4
50	121.18.238.125
48	115.238.245.8
36	122.226.181.166
24	5.188.10.156
21	77.72.82.11
20	198.15.152.102
17	181.214.87.221
15	103.75.189.121
12	5.101.0.9
12	58.210.182.86
12	43.243.123.227
11	103.99.2.3
10	60.164.208.135
10	139.162.110.42

Figure4: attack Count in Elsa



INTERVAL: 2018-02-16 00:00:00 -> 2018-02-16 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 0.9% 60.0% 39.1%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	265
total events	435
total signatures	10

PRIORITY

high	4 (0.9%)
medium	261 (60.0%)
low	170 (39.1%)
other	-

CLASSIFICATION

🟥 compromised L1	170 (39.1%)
🟧 compromised L2	-
🟧 attempted access	-
🟨 denial of service	-
🟪 policy violation	-
🟨 reconnaissance	-
🟪 malicious	-
🟦 no action req'd.	-
🟥 escalated event	-

TAGS

no tags

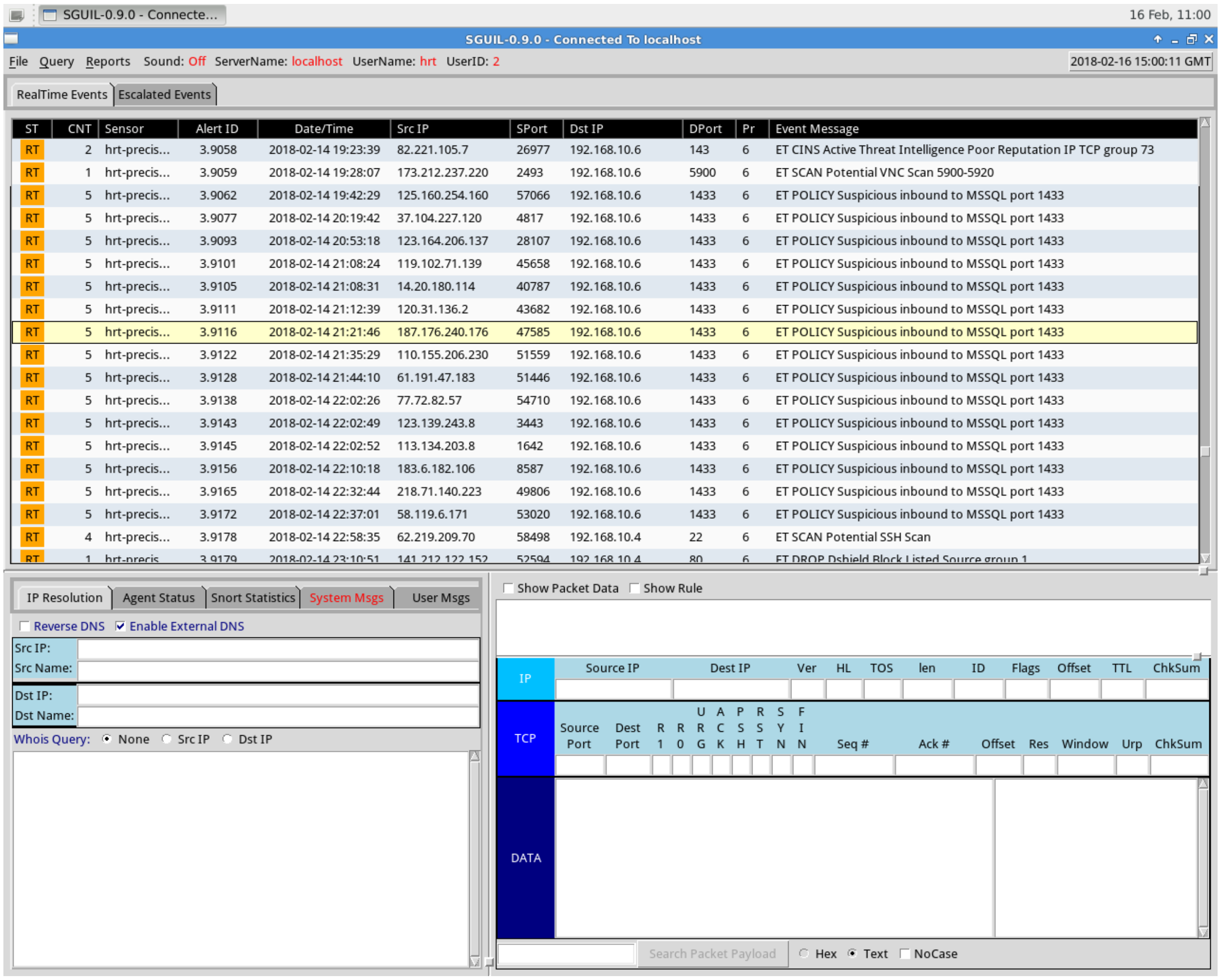
HISTORY

ET POLICY Suspicious inbound to M..
ET DROP Dshield Block Listed Sour..
ET SCAN LibSSH Based Frequent SSH..(2)
ET SCAN SSH BruteForce Tool with ..
ET SCAN Potential SSH Scan(5)

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
2	1	1		14:59:38	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 40	2500078	6	**0.460%**
10	2	1		14:43:46	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	**2.299%**
225	45	1		14:37:18	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	**51.724%**
7	3	1		12:28:04	ET SCAN Potential SSH Scan	2001219	6	**1.609%**
1	1	1		11:28:36	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 3	2403304	6	**0.230%**
8	7	1		11:04:25	ET SCAN Potential VNC Scan 5900-5920	2002911	6	**1.839%**
1	1	1		09:53:29	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 89	2403476	6	**0.230%**
1	1	1		09:33:08	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 54	2500106	6	**0.230%**
6	5	2		08:25:09	ET DROP Dshield Block Listed Source group 1	2402000	6	**1.379%**
4	1	1		00:18:12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	2006546	6	**0.920%**

WELCOME **hrt** | LOGOUT UTC **15:01:48**

Figure5: Squert tools



Sound: Off ServerName: localhost UserName: hrt UserID: 2

2018-02-16 15:00:11 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	hrt-precis...	3.9058	2018-02-14 19:23:39	82.221.105.7	26977	192.168.10.6	143	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 73
RT	1	hrt-precis...	3.9059	2018-02-14 19:28:07	173.212.237.220	2493	192.168.10.6	5900	6	ET SCAN Potential VNC Scan 5900-5920
RT	5	hrt-precis...	3.9062	2018-02-14 19:42:29	125.160.254.160	57066	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9077	2018-02-14 20:19:42	37.104.227.120	4817	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9093	2018-02-14 20:53:18	123.164.206.137	28107	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9101	2018-02-14 21:08:24	119.102.71.139	45658	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9105	2018-02-14 21:08:31	14.20.180.114	40787	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9111	2018-02-14 21:12:39	120.31.136.2	43682	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9116	2018-02-14 21:21:46	187.176.240.176	47585	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9122	2018-02-14 21:35:29	110.155.206.230	51559	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9128	2018-02-14 21:44:10	61.191.47.183	51446	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9138	2018-02-14 22:02:26	77.72.82.57	54710	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9143	2018-02-14 22:02:49	123.139.243.8	3443	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9145	2018-02-14 22:02:52	113.134.203.8	1642	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9156	2018-02-14 22:10:18	183.6.182.106	8587	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9165	2018-02-14 22:32:44	218.71.140.223	49806	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	5	hrt-precis...	3.9172	2018-02-14 22:37:01	58.119.6.171	53020	192.168.10.6	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	4	hrt-precis...	3.9178	2018-02-14 22:58:35	62.219.209.70	58498	192.168.10.4	22	6	ET SCAN Potential SSH Scan
RT	1	hrt-precis...	3.9179	2018-02-14 23:10:51	141.212.122.152	52594	192.168.10.4	80	6	ET DROP Dshield Block Listed Source group 1

□ Reverse DNS ☑ Enable External DNS

Whois Query: ● None ○ Src IP ○ Dst IP

□ Show Packet Data □ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum

○ Hex ● Text □ NoCase

Figure6: SGUIL tools

Based on IP T-POT approximate locations of IP address which is presented on Figure 7 most of the attacks are from Russia as showcased by the red dot.

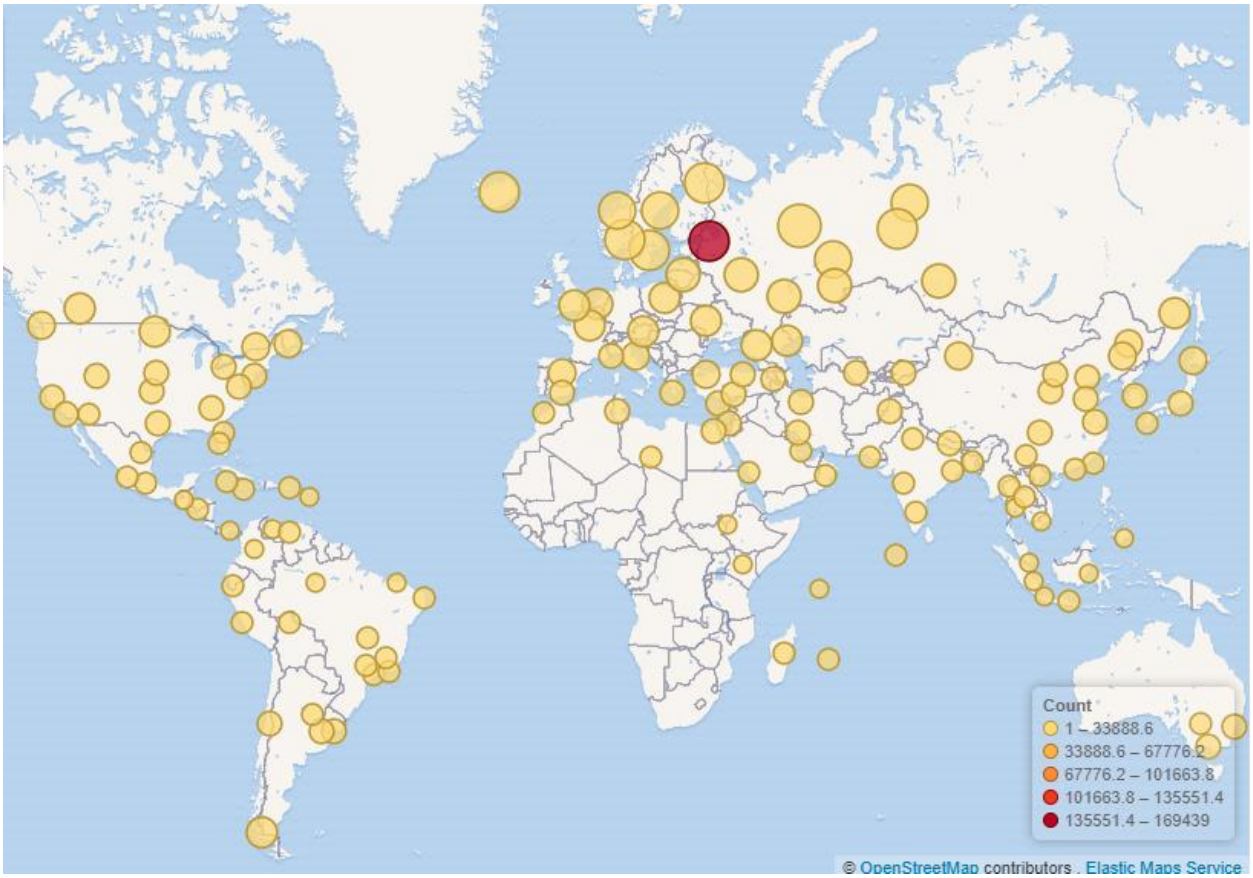


Figure7: The approximate locations of the IP addresses

Based on T-POT 91% of attacks are from addresses with a bad reputation, while only 8.94% are fom known attackers (figure8).

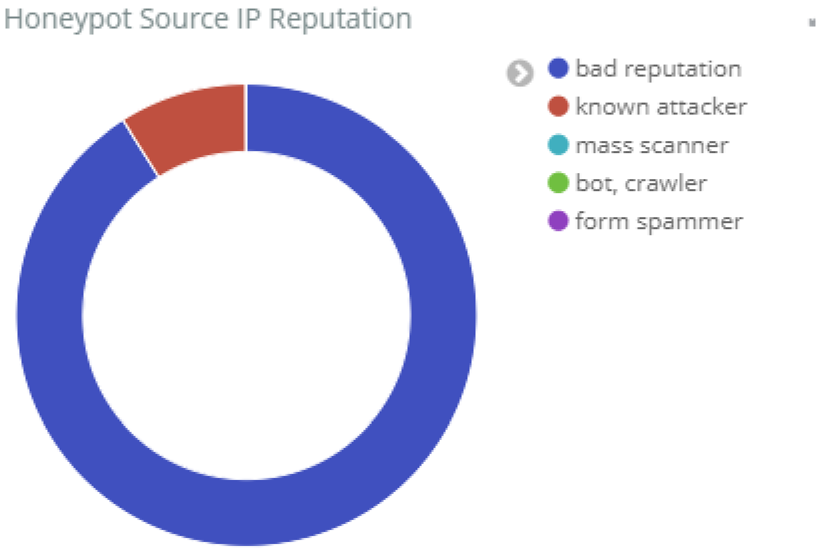


Figure8: Hoenypot source IP Reputation

4.2 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:

Table4: common username used by attackers

username	Number of occurrence
admin	49906
root	21523
1234	8184
enable	1976
shell	1923
guest	963
default	623
supervisor	599
support	420
user	368

Table5: common password used by attackers

password	Number of occurrence
No password	43865
1234	9416
system	1977
sh	1923
admin	1037
12345	949
password	902
123456	685
7ujMko0admin	644
1111	613

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

Table6: common command used by attackers

	command	Number of occurrence
1	ls	8
2	Running their code	3
3	Unkown command from Bots	2

We are dealing with a kind of Bot which uses the above code 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.

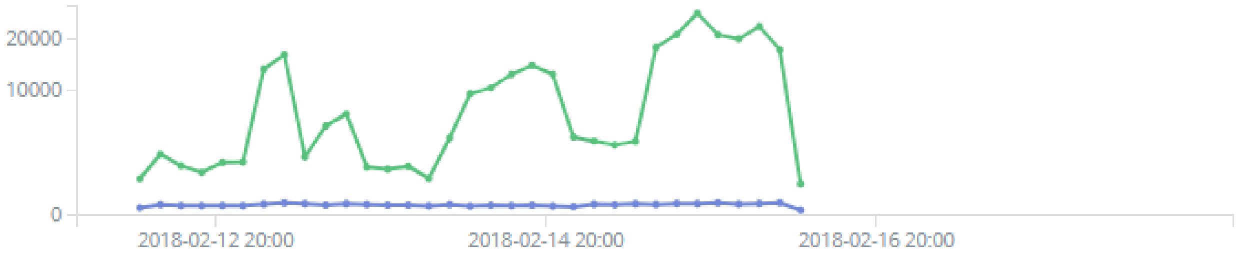
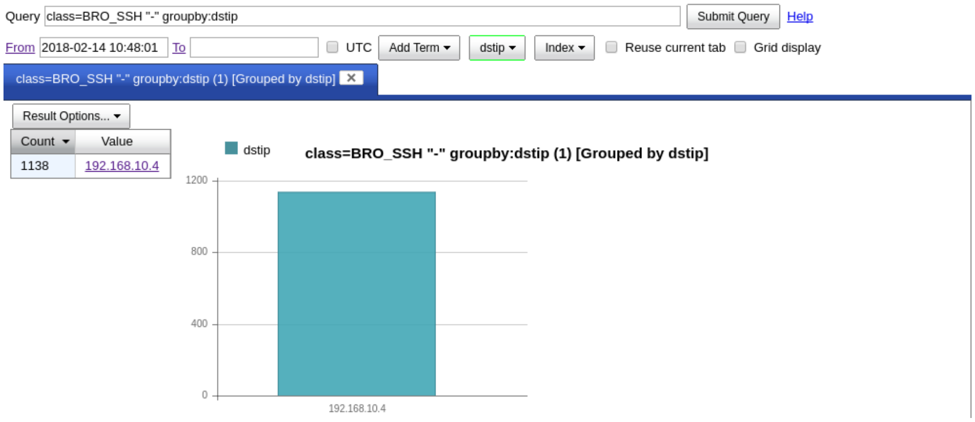


Figure9: Hoenypot attack based on time

4.5 Inside Network

Inside Network activities which are logged by **Security Onion** are shown in figures 10, 11 and 12. This traffic includes http, ftp, SSH, and system logs.



Query class=BRO_SSH "-" groupby:dstip

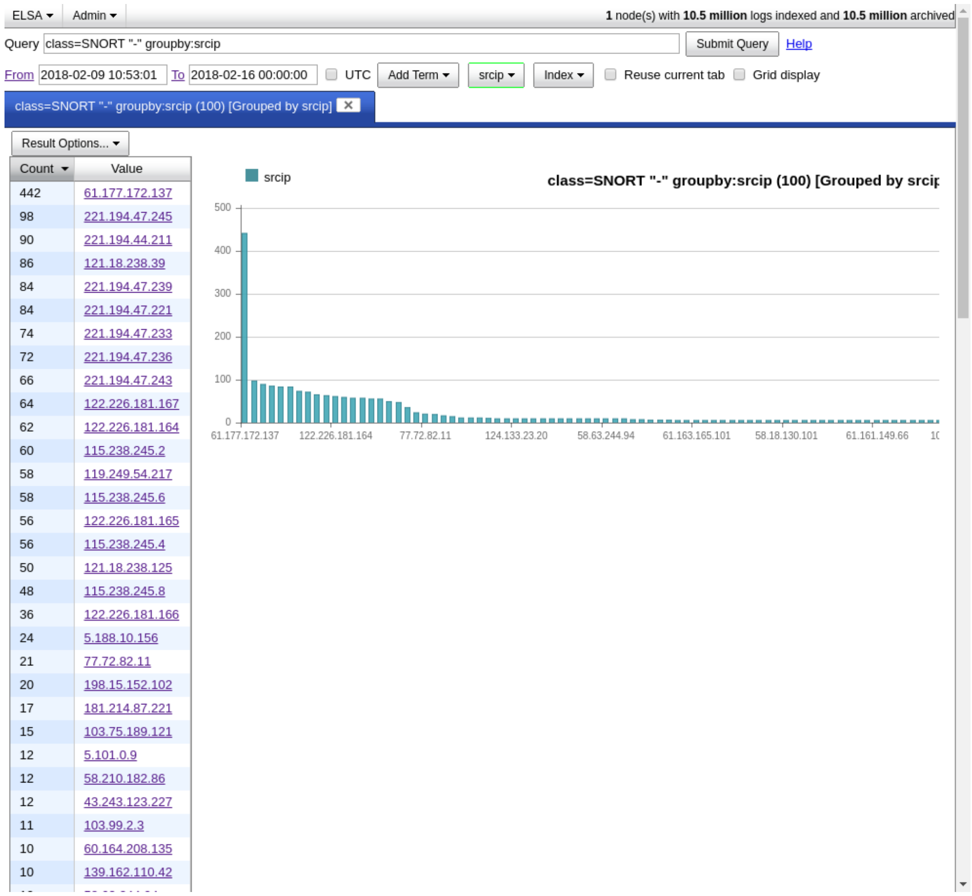
From 2018-02-14 10:48:01 To

□ UTC

class=BRO_SSH "-" groupby:dstip (1) [Grouped by dstip]

Count	Value
1138	192.168.10.4

Figure10: TOP SSH PORT



1 node(s) with **10.5 million** logs indexed and **10.5 million** archived

Query class=SNORT "-" groupby:srcip

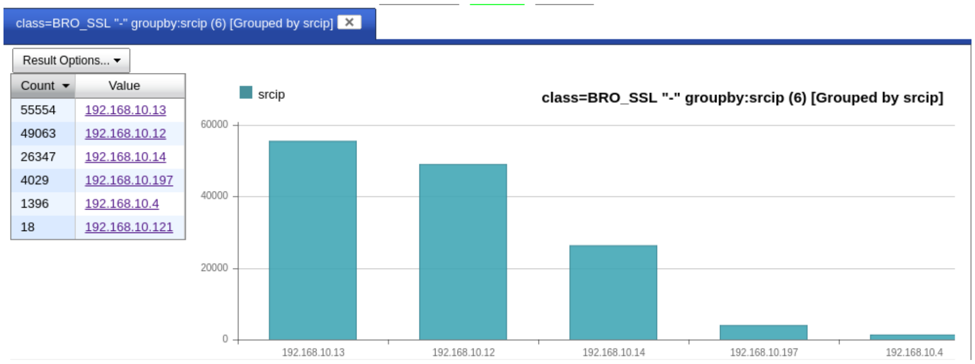
From 2018-02-09 10:53:01 To 2018-02-16 00:00:00

□ UTC

class=SNORT "-" groupby:srcip (100) [Grouped by srcip]

Count	Value
442	61.177.172.137
98	221.194.47.245
90	221.194.44.211
86	121.18.238.39
84	221.194.47.239
84	221.194.47.221
74	221.194.47.233
72	221.194.47.236
66	221.194.47.243
64	122.226.181.167
62	122.226.181.164
60	115.238.245.2
58	119.249.54.217
58	115.238.245.6
56	122.226.181.165
56	115.238.245.4
50	121.18.238.125
48	115.238.245.8
36	122.226.181.166
24	5.188.10.156
21	77.72.82.11
20	198.15.152.102
17	181.214.87.221
15	103.75.189.121
12	5.101.0.9
12	58.210.182.86
12	43.243.123.227
11	103.99.2.3
10	60.164.208.135
10	139.162.110.42

Figure11: TOP Destination IP from Local Users



class=BRO_SSL "-" groupby:srcip (6) [Grouped by srcip] ✕

Result Options... ▾

Count ▾	Value
55554	192.168.10.13
49063	192.168.10.12
26347	192.168.10.14
4029	192.168.10.197
1396	192.168.10.4
18	192.168.10.121

Figure12: TOP Local Users