Honeynet Weekly Report
Canadian Institute for Cybersecurity (CIC)

Report(3) Capture: 01-02-2018 to 08-02-2018

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 the CIC-Honeynet dataset, we have defined a separated network with these services:

- Email Server(SMTP-IMAP)
- FTP Server
- File Server
- Web Server (Apache:WordPress-MySql)
- SSH(Kippo)
- Http
- Https

Inside the network there are ‘like’ real users. Each user has real behaviors and surfs the Internet based on the above protocols. 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 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.

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, bots when they want to produce spams we can grab these spams through “Contact Form 7 Honeypot”(Figure 1).

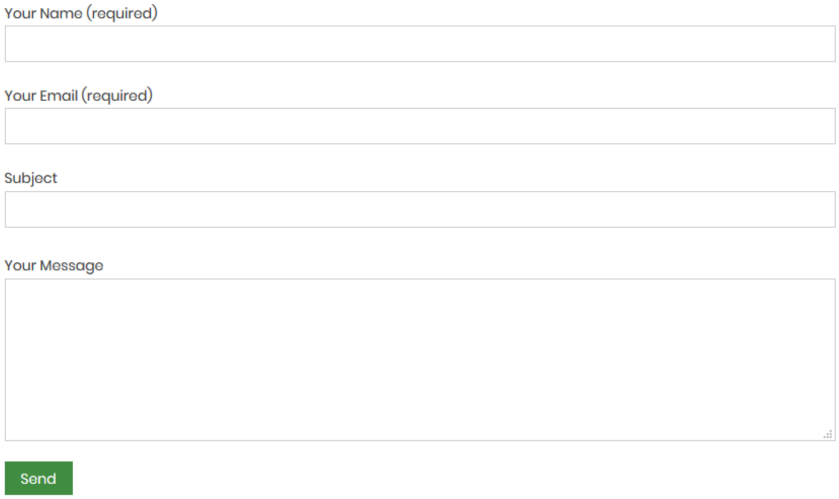


Figure1: Contact Form 7 Honeypot

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 analysing traffic on the edge of 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

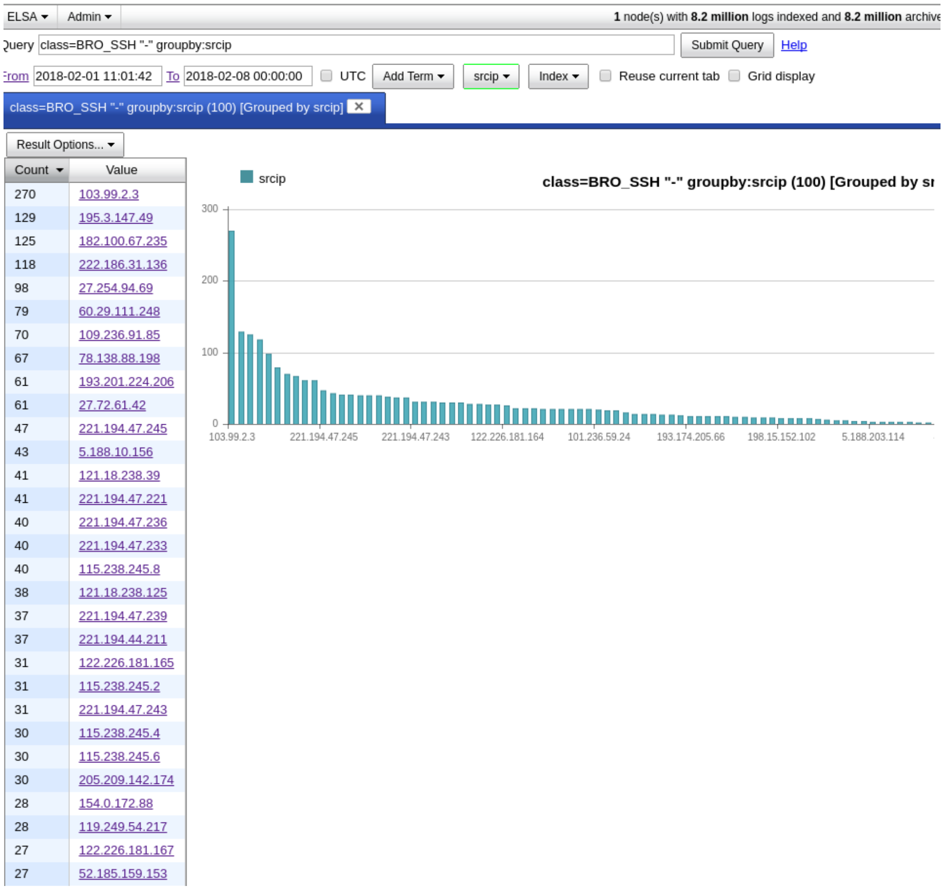
We analyzed the IP addresses that made login attempts using the Domain Bulk look IP , We received login attempts from 101 unique IP addresses in 32 countries; the breakdown by country is shown in table 1.

Table1: IP breakdown by country

IP	Country	Number of Attack
103.99.2.3	Vietnam	270
195.3.147.49	Latvia	129
182.100.67.235	China	125
222.186.31.136	China	118
27.254.94.69	Thailand	98
60.29.111.248	China	79
109.236.91.85	Netherlands	70
78.138.88.198	Germany	67
27.72.61.42	Vietnam	61
193.201.224.206	Ukraine	61
221.194.47.245	China	47
5.188.10.156	Croatia	43
221.194.47.221	China	41
121.18.238.39	China	41

IP	Country	Number of Attack
115.238.245.8	China	40
221.194.47.233	China	40
221.194.47.236	China	40
121.18.238.125	China	38
221.194.44.211	China	37
221.194.47.239	China	37
221.194.47.243	China	31
115.238.245.2	China	31
122.226.181.165	China	31
205.209.142.174	United States	30
115.238.245.6	China	30
115.238.245.4	China	30

This list is proved by our **Security Onion**, which is demonstrated in Figure2. Also we can prove it in Squert and SGUIL which are tools of Security Onion to exactly detect attackers. For example in Figure3 and Figure 4, we evaluate 115.238.245.4 IP address and as it is demonstrated in Figure2,3,4 all tools detect this IP address as a brute force attack.



1 node(s) with **8.2 million** logs indexed and **8.2 million** archive

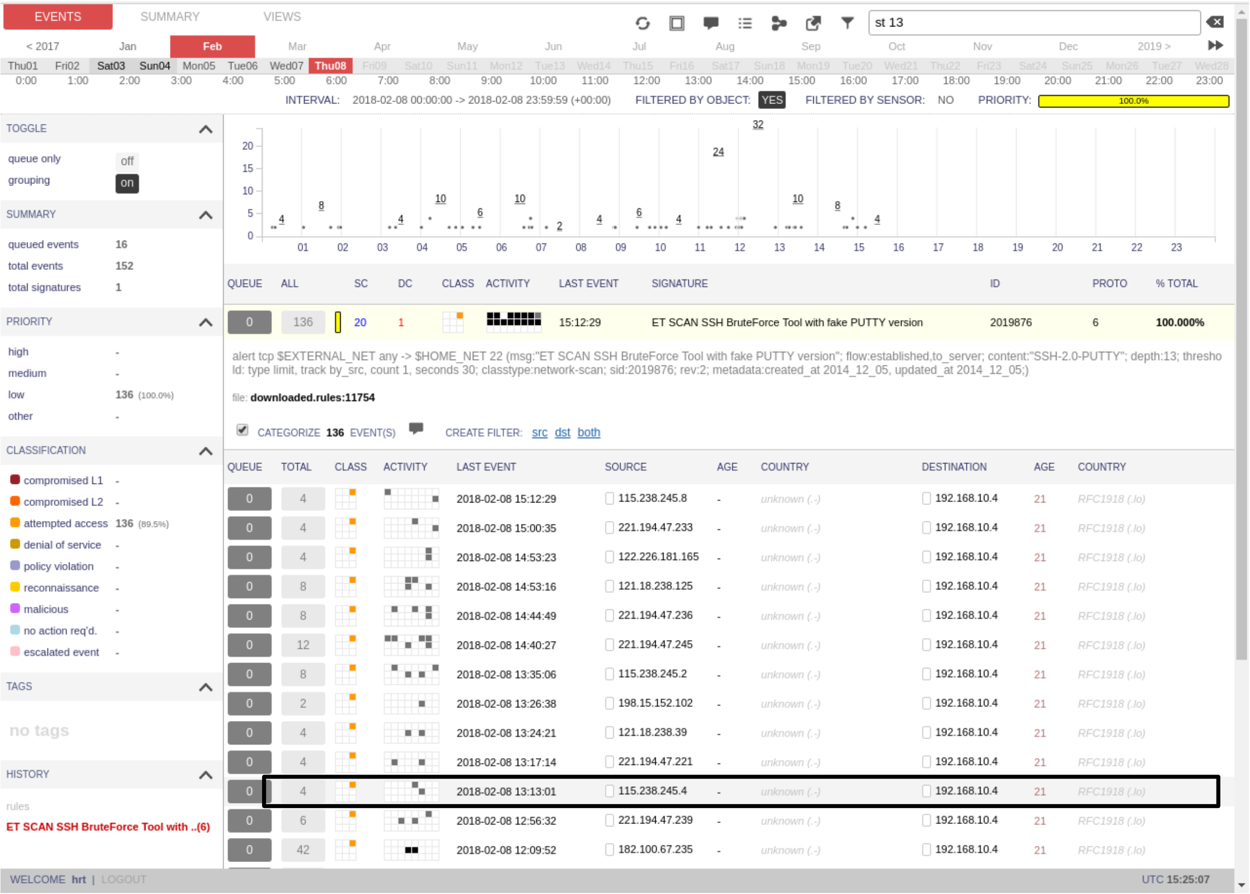
Query class=BRO_SSH "-" groupby:srcip

From 2018-02-01 11:01:42 To 2018-02-08 00:00:00 □ UTC □ Reuse current tab □ Grid display

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

Count ▾	Value
270	103.99.2.3
129	195.3.147.49
125	182.100.67.235
118	222.186.31.136
98	27.254.94.69
79	60.29.111.248
70	109.236.91.85
67	78.138.88.198
61	193.201.224.206
61	27.72.61.42
47	221.194.47.245
43	5.188.10.156
41	121.18.238.39
41	221.194.47.221
40	221.194.47.236
40	221.194.47.233
40	115.238.245.8
38	121.18.238.125
37	221.194.47.239
37	221.194.44.211
31	122.226.181.165
31	115.238.245.2
31	221.194.47.243
30	115.238.245.4
30	115.238.245.6
30	205.209.142.174
28	154.0.172.88
28	119.249.54.217
27	122.226.181.167
27	52.185.159.153

Figure2: attack Count in Elsa



INTERVAL: 2018-02-08 00:00:00 -> 2018-02-08 23:59:59 (+00:00) FILTERED BY OBJECT: YES FILTERED BY SENSOR: NO PRIORITY: 100.0%

TOGGLE

queue only off
grouping on

SUMMARY

queued events	16
total events	152
total signatures	1

PRIORITY

high	-
medium	-
low	136 (100.0%)
other	-

CLASSIFICATION

compromised L1	-
compromised L2	-
attempted access	136 (89.5%)
denial of service	-
policy violation	-
reconnaissance	-
malicious	-
no action req'd.	-
escalated event	-

TAGS

no tags

HISTORY

rules
ET SCAN SSH BruteForce Tool with ..(6)

QUEUE	ALL	SC	DC	CLASS	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
0	136	20	1			15:12:29	ET SCAN SSH BruteForce Tool with fake PUTTY version	2019876	6	100.000%

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN SSH BruteForce Tool with fake PUTTY version"; flow:established,to_server; content:"SSH-2.0-PUTTY"; depth:13; thresho
ld: type limit, track by_src, count 1, seconds 30; classtype:network-scan; sid:2019876; rev:2; metadata:created_at 2014_12_05, updated_at 2014_12_05;)
```

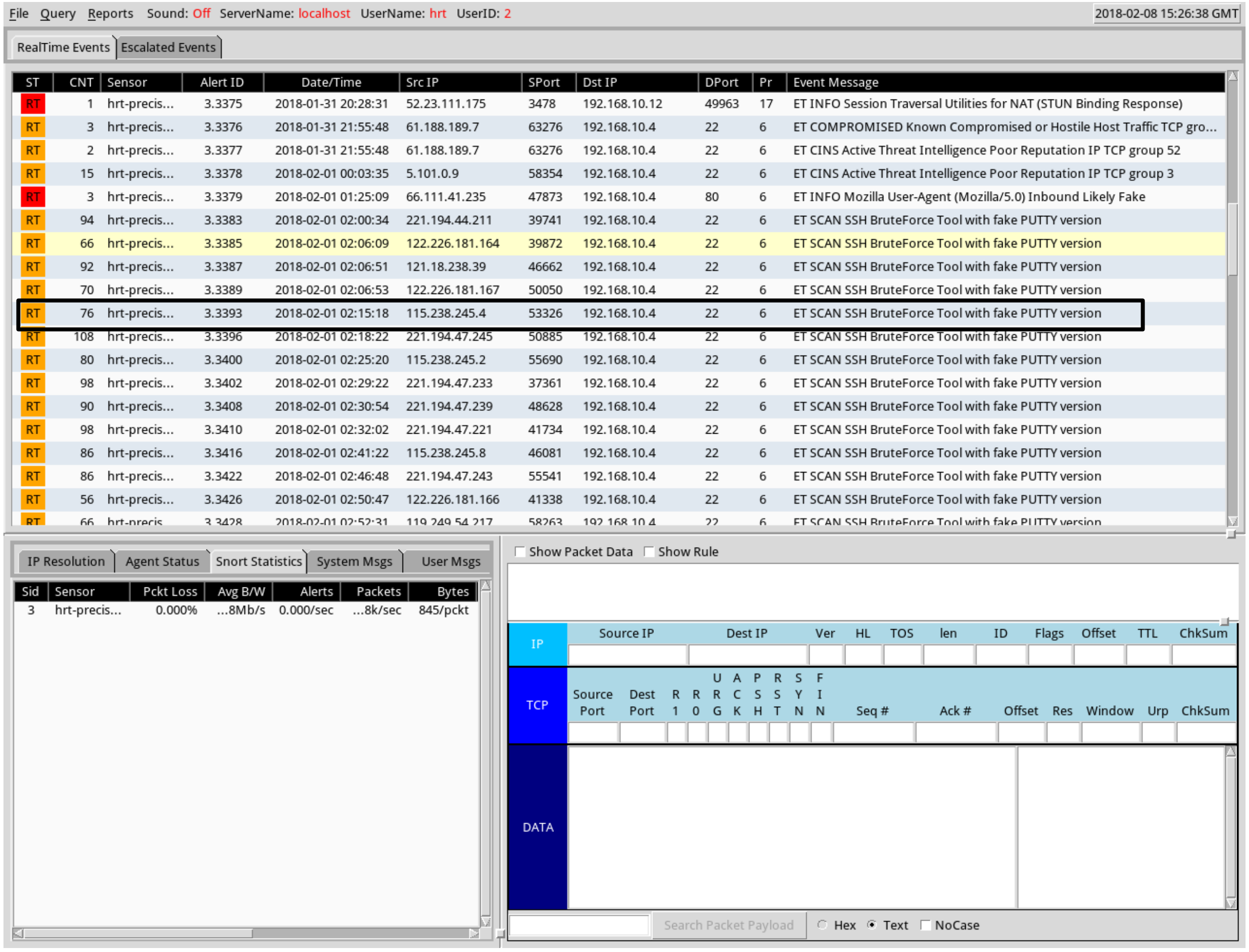
file: **downloaded.rules:11754**

☑ CATEGORIZE **136** EVENT(S) CREATE FILTER: src dst both

QUEUE	TOTAL	CLASS	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
0	4			2018-02-08 15:12:29	□ 115.238.245.8	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	4			2018-02-08 15:00:35	□ 221.194.47.233	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	4			2018-02-08 14:53:23	□ 122.226.181.165	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	8			2018-02-08 14:53:16	□ 121.18.238.125	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	8			2018-02-08 14:44:49	□ 221.194.47.236	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	12			2018-02-08 14:40:27	□ 221.194.47.245	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	8			2018-02-08 13:35:06	□ 115.238.245.2	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	2			2018-02-08 13:26:38	□ 198.15.152.102	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	4			2018-02-08 13:24:21	□ 121.18.238.39	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	4			2018-02-08 13:17:14	□ 221.194.47.221	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	4			2018-02-08 13:13:01	□ 115.238.245.4	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	6			2018-02-08 12:56:32	□ 221.194.47.239	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)
0	42			2018-02-08 12:09:52	□ 182.100.67.235	-	unknown (.-)	□ 192.168.10.4	21	RFC1918 (.lo)

WELCOME hrt | LOGOUT UTC 15:25:07

Figure3: Squert tools



File Query Reports Sound: Off ServerName: localhost UserName: hrt UserID: 2 2018-02-08 15:26:38 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	hrt-precis...	3.3375	2018-01-31 20:28:31	52.23.111.175	3478	192.168.10.12	49963	17	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)
RT	3	hrt-precis...	3.3376	2018-01-31 21:55:48	61.188.189.7	63276	192.168.10.4	22	6	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP gro...
RT	2	hrt-precis...	3.3377	2018-01-31 21:55:48	61.188.189.7	63276	192.168.10.4	22	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 52
RT	15	hrt-precis...	3.3378	2018-02-01 00:03:35	5.101.0.9	58354	192.168.10.4	22	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 3
RT	3	hrt-precis...	3.3379	2018-02-01 01:25:09	66.111.41.235	47873	192.168.10.4	80	6	ET INFO Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
RT	94	hrt-precis...	3.3383	2018-02-01 02:00:34	221.194.44.211	39741	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	66	hrt-precis...	3.3385	2018-02-01 02:06:09	122.226.181.164	39872	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	92	hrt-precis...	3.3387	2018-02-01 02:06:51	121.18.238.39	46662	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	70	hrt-precis...	3.3389	2018-02-01 02:06:53	122.226.181.167	50050	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	76	hrt-precis...	3.3393	2018-02-01 02:15:18	115.238.245.4	53326	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	108	hrt-precis...	3.3396	2018-02-01 02:18:22	221.194.47.245	50885	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	80	hrt-precis...	3.3400	2018-02-01 02:25:20	115.238.245.2	55690	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	98	hrt-precis...	3.3402	2018-02-01 02:29:22	221.194.47.233	37361	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	90	hrt-precis...	3.3408	2018-02-01 02:30:54	221.194.47.239	48628	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	98	hrt-precis...	3.3410	2018-02-01 02:32:02	221.194.47.221	41734	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	86	hrt-precis...	3.3416	2018-02-01 02:41:22	115.238.245.8	46081	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	86	hrt-precis...	3.3422	2018-02-01 02:46:48	221.194.47.243	55541	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	56	hrt-precis...	3.3426	2018-02-01 02:50:47	122.226.181.166	41338	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	66	hrt-precis	3.3428	2018-02-01 02:52:31	119.249.54.217	58263	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

Sid	Sensor	Pckt Loss	Avg B/W	Alerts	Packets	Bytes
3	hrt-precis...	0.000%	...8Mb/s	0.000/sec	...8k/sec	845/pckt

□ Show Packet Data □ Show Rule

Figure4: SGUIL tools

Based on IP and with using GEO location tools, we can demonstrate approximate locations of IP address which is presented on Figure 5.

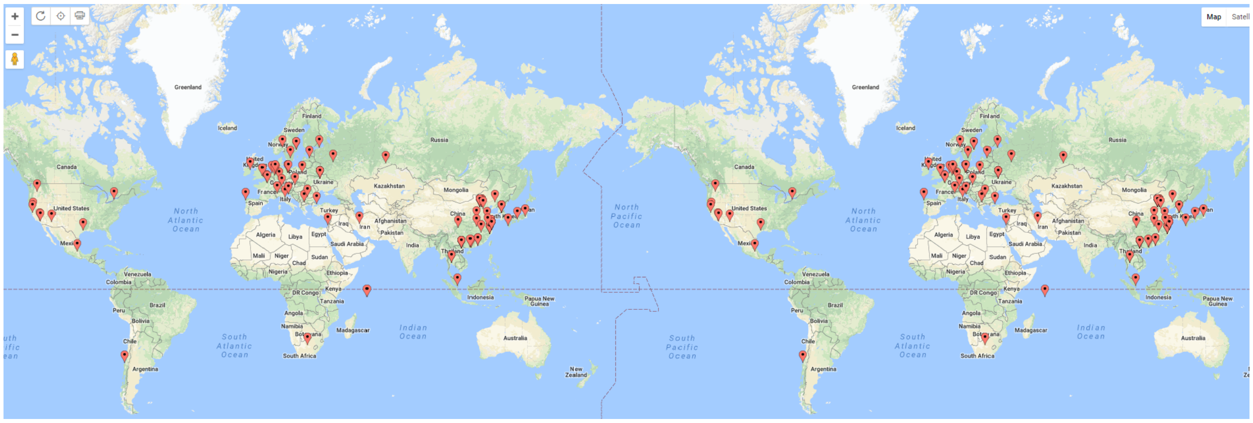


Figure5: The approximate locations of the IP addresses

Based on Untangle firewall report, from 1500 sessions, around 87% of sessions are on SSH, 1% on FTP, 10% on HTTP and finally 2% is on POP3 (Figure 6).

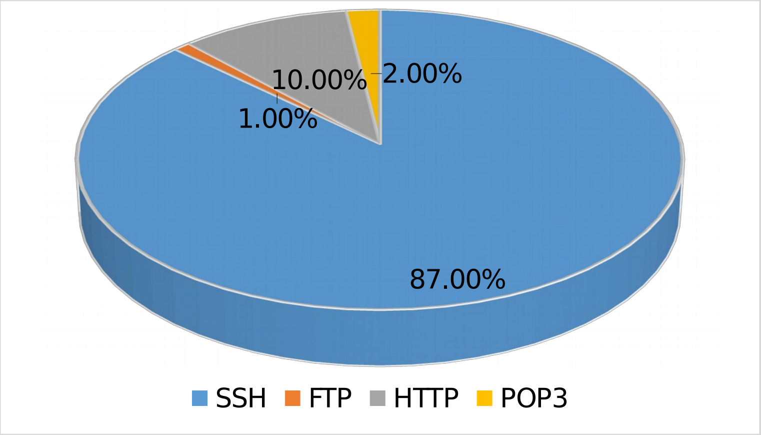


Figure6: top sessions ports

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:

Table2: common username used by attackers

	username	Number of occurrence
1	root	4831
2	admin	954
3	user	765
4	pi	117
5	support	49

Table3: common password used by attackers

	password	Number of occurrence
1	123	2077
2	1234	1315
3	123456	192
4	password	122

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	ls	10
2	Running their code	4
3	Unkown command from Bots	3

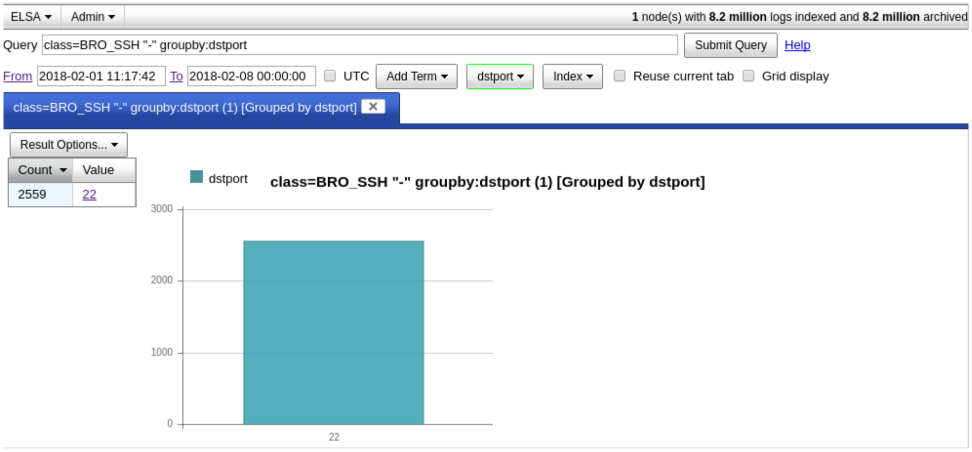
We are dealing with a kind of Bot which uses the above commands to change the file system. (All executed commands by Bots through SSH are available in captured data)

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 7, 8 and 9. This traffic includes http, ftp, SSH, and system logs.



1 node(s) with **8.2 million** logs indexed and **8.2 million** archived

Query class=BRO_SSH "-" groupby:dstport

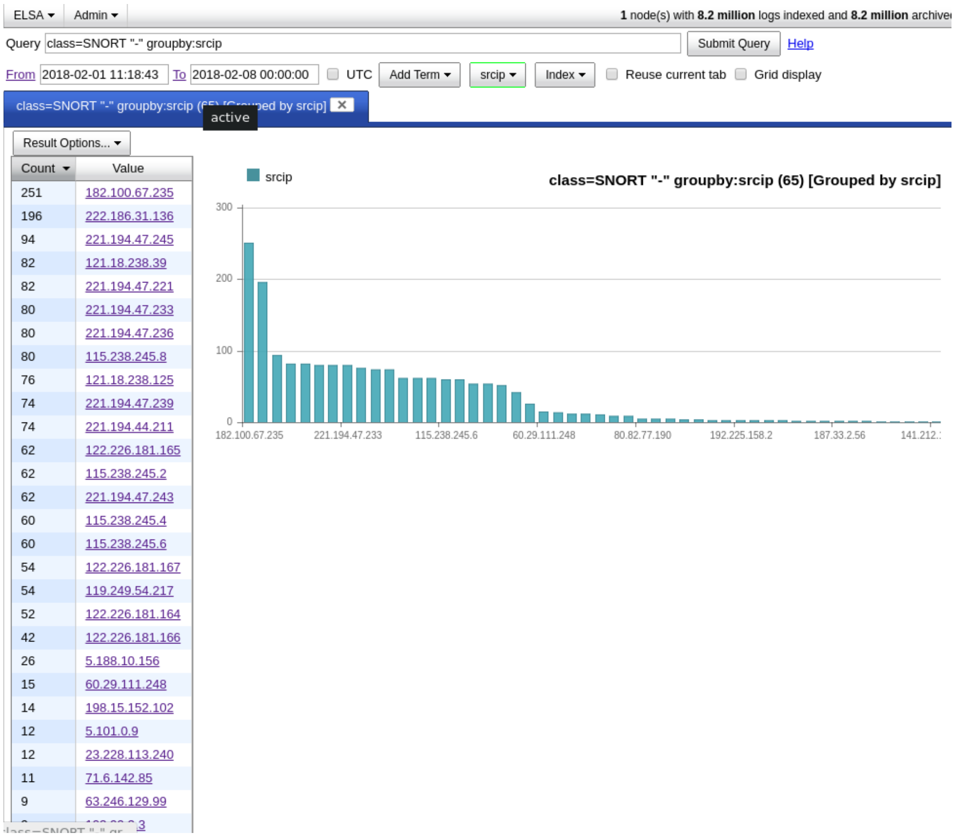
From 2018-02-01 11:17:42 To 2018-02-08 00:00:00

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

Count	Value
2559	22

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

Figure7: TOP SSH PORT



1 node(s) with **8.2 million** logs indexed and **8.2 million** archive

Query: class=SNORT "-" groupby:srcip

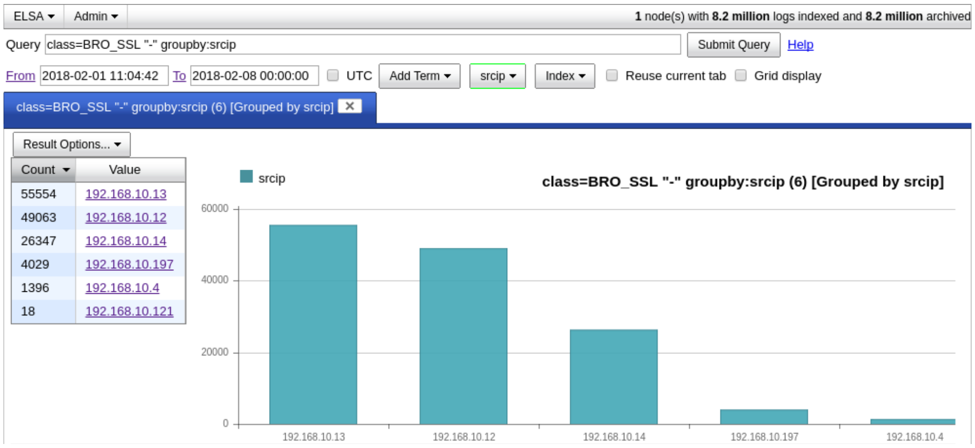
From 2018-02-01 11:18:43 To 2018-02-08 00:00:00 □ UTC □ Reuse current tab □ Grid display

class=SNORT "-" groupby:srcip (65) [Grouped by srcip] ✕

class=SNORT "-" groupby:srcip (65) [Grouped by srcip]

Count ▾	Value
251	182.100.67.235
196	222.186.31.136
94	221.194.47.245
82	121.18.238.39
82	221.194.47.221
80	221.194.47.233
80	221.194.47.236
80	115.238.245.8
76	121.18.238.125
74	221.194.47.239
74	221.194.44.211
62	122.226.181.165
62	115.238.245.2
62	221.194.47.243
60	115.238.245.4
60	115.238.245.6
54	122.226.181.167
54	119.249.54.217
52	122.226.181.164
42	122.226.181.166
26	5.188.10.156
15	60.29.111.248
14	198.15.152.102
12	5.101.0.9
12	23.228.113.240
11	71.6.142.85
9	63.246.129.99

Figure8: TOP Destination IP from Local Users



1 node(s) with **8.2 million** logs indexed and **8.2 million** archived

Query: class=BRO_SSL "-" groupby:srcip

From 2018-02-01 11:04:42 To 2018-02-08 00:00:00 □ UTC □ Reuse current tab □ Grid display

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

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

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

Figure9: TOP Local Users