Honeynet Weekly Report
Canadian Institute for Cybersecurity (CIC)

Report(6) Captured from 24-02-2018 to 09-03-2018

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)(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. In the inside network, we put **pfsense** firewall at the edge of network and NAT different services for public users. There is a firewall that some ports such as 20, 21, 22, 53, 80, 143, 443 are opened intentionally to capture and absorb attackers behaviours. 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, when the bots want to produce spams, we can grab these spams through “Contact Form 7 Honeypot”(Figure 1).

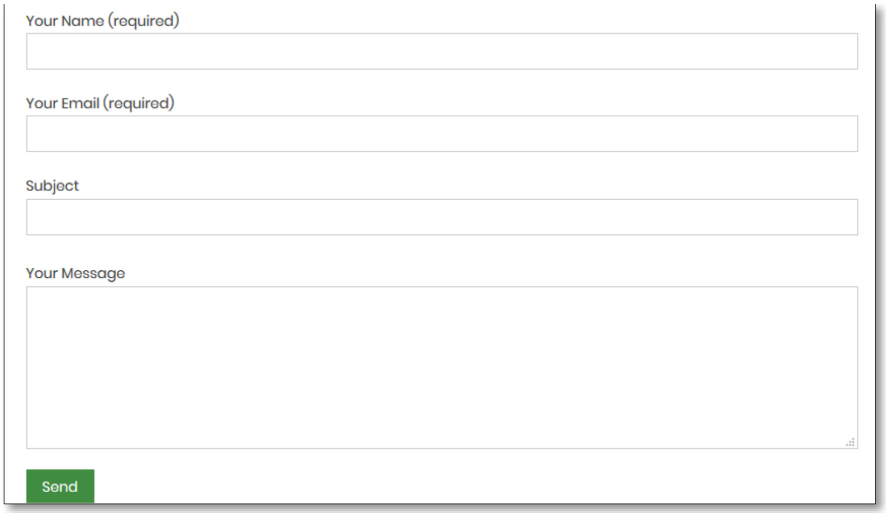


Figure1: Contact Form 7 Honeypot

CIC-honeynet uses T-POT tool outside firewall which is equipped with several tools. T-Pot is based on well-established honeypot daemons which includes 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 in order 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 CIC-honeynet and installed 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 **pfsense** firewall in the internal network Security Onion has been used to analyse 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 3 PCs are running the CIC-Benign behaviour generator (an in house developed agent), includes internet surfing, FTP uploading and downloading, and Emailing activities. 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.

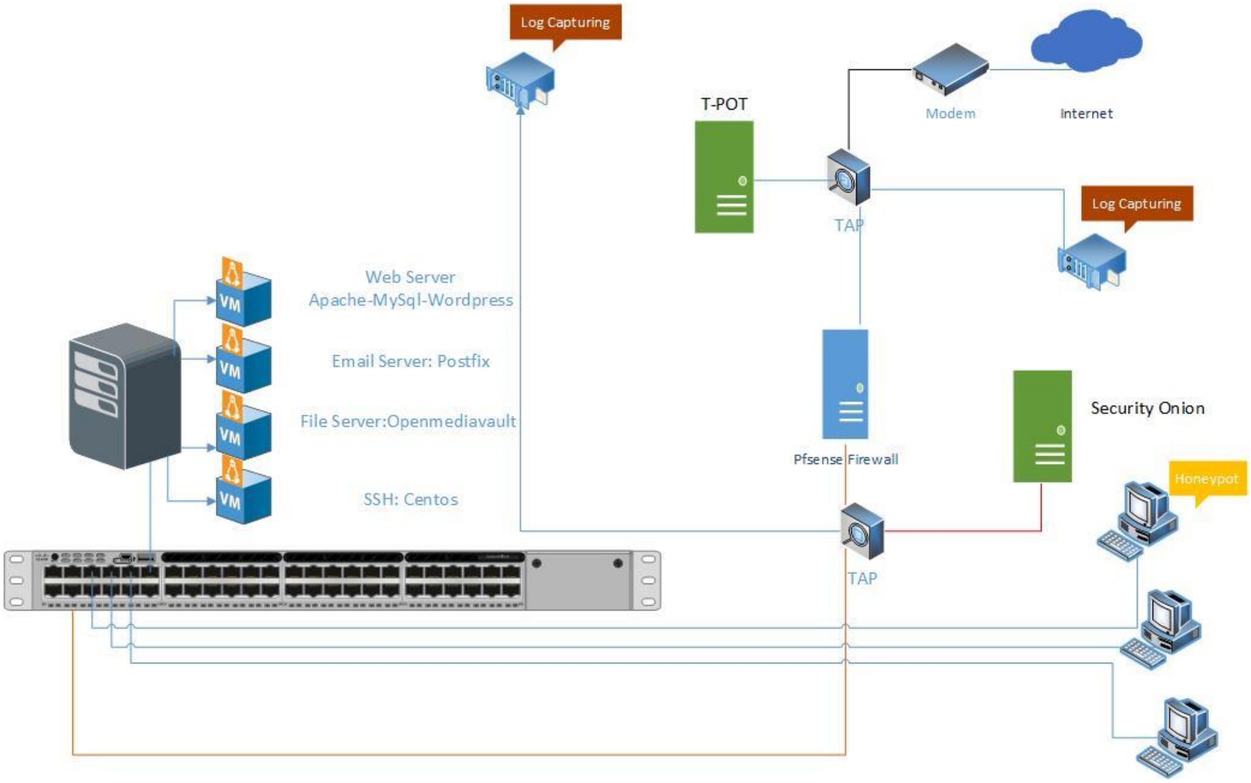


Figure2: Network Diagram

All traffic captured through the internal-TAP and external-TAP and analysis by **CICFlowMeter** which extracts more than 80 traffic features. The source code of CICFlowMeter is available in GitHub.

Also we used **Kippo tools** to mimic the SSH command inside the firewall and captures the users commands. Some easy password such as 1234, 123… are entered in Kippo database to make it vulnerable for attackers.

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 recieved login attempts from are listed in Table 1.

Table1: IP breakdown by country

Country	Number of Attack
Russia	843602
United States	209589
China	109581
Netherlands	62931
Brazil	56486
Colombia	43542
Israel	32443
Germany	24182
France	22287
Ukraine	19932

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
69.197.135.10	91323
109.248.9.101	80844
109.248.9.102	67838
5.188.86.214	56877
61.177.172.232	56037
190.0.20.202	43412
5.188.86.170	36963
5.188.86.169	32571
5.188.86.209	31748

In figure3, top 5 of countries are demonstrated by related ports. For example the attacks from Russia have been 94.96% through port 2222, 1.92% through port 25, 2.26% through port 443, and 0.49% through port 80.

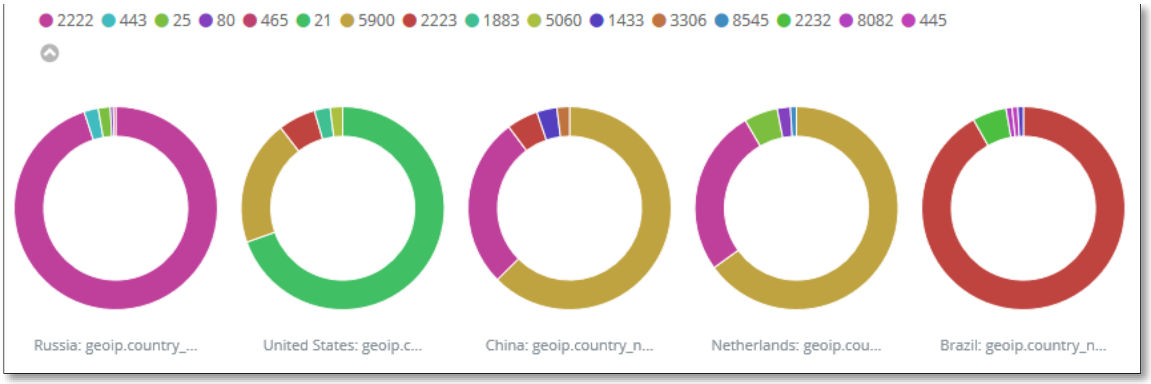


Figure3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

During this week, we had two CVEs namely, CVE-2003-0567 and CVE-2017-0143 which the number of attacks for each CVE are demonstrated in Table3.

Table3: Top 10 Source IP

CVE-ID	Numbers
CVE-2003-0567	47166
CVE-2017-0143	28

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

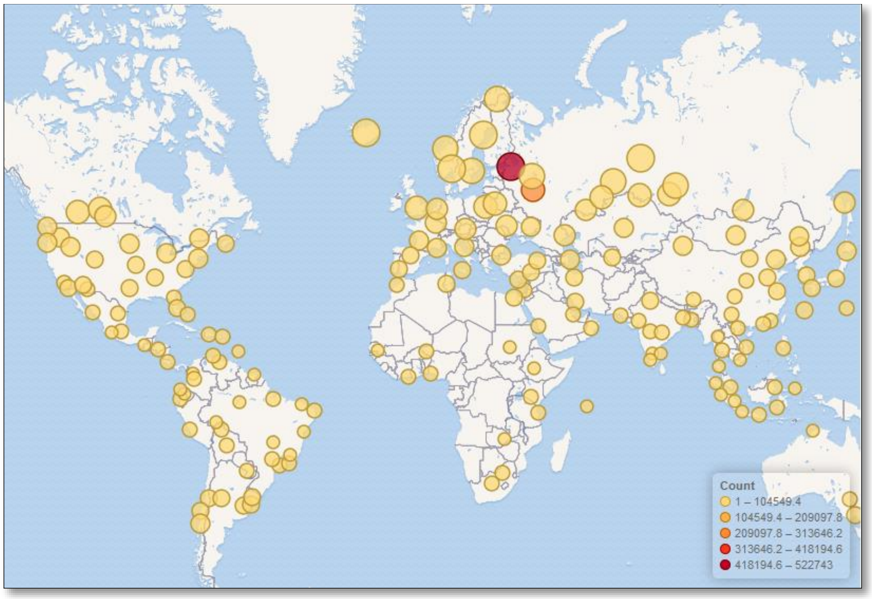


Figure4: The approximate locations of the IP addresses

Based on T-POT the 81.43% of attacks are from addresses with a bad reputation, while only 18.46% are from known attackers (figure5).

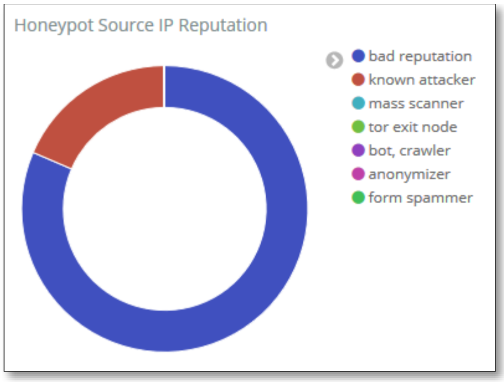


Figure5: External Honeypot source IP Reputation

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

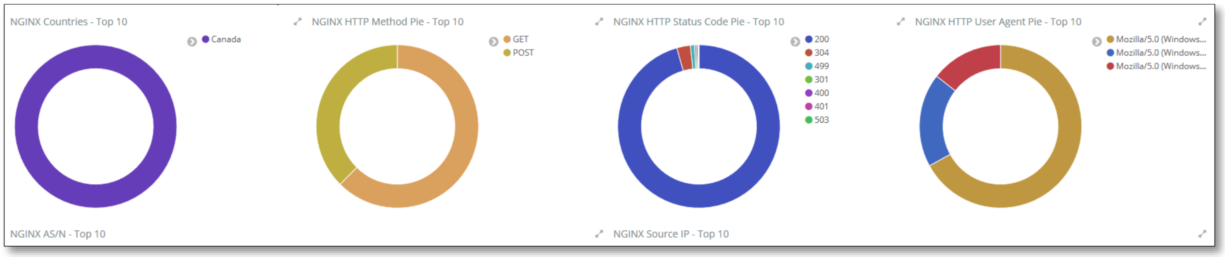


Figure6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4 which around 24304 of them are from Global Frag Networks.

Table4: Top 10 Source IP of VNC attack

username	Number of occurrence
107.179.25.209	23680
222.186.174.93	19700
185.70.187.155	14736
185.222.210.22	10439
123.249.12.230	6110
194.28.112.157	5363
104.247.201.3	977

3.3 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:

Table5: common username used by attackers

username	Number of occurrence
root	170041
0	153924
admin	75750
1234	14379
[blank]	12217
enable	7080
shell	6908
user	3630
guest	3626
Administrator	3296

Table6: common password used by attackers

password	Number of occurrence
[blank]	189258
1234	22189
[blank][blank]	20026
system	6708
sh	6536
admin	6237
password	6093
123456	5204
12345	4424
user	3515

3.4 TOP Commands

Table 7 and 8, show the most common commands used by attackers in Cowrie and Mailoney external honeypots. (All commands are available in captured data)

Table7: common command used by attackers grabbed by Cowrie

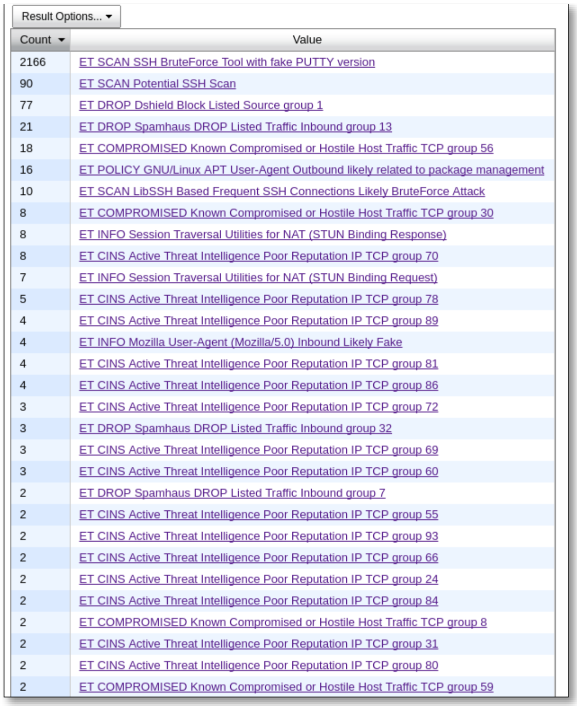
	command	Number of occurrence
1	/gweerwe323f	63
2	cat /proc/cpuinfo	40
3	free -m	36
4	ps -x	36
5	export HISTFILE=/dev/null	29

Table8: common command used by attackers grabbed by Mailoney

	command	Number of occurrence
1	AUTH LOGIN	867
2	EHLO MAIL03SH-PC	811
3	EHLO User	144
4	QUIT	57
5	EHLO 205.174.165.74	3

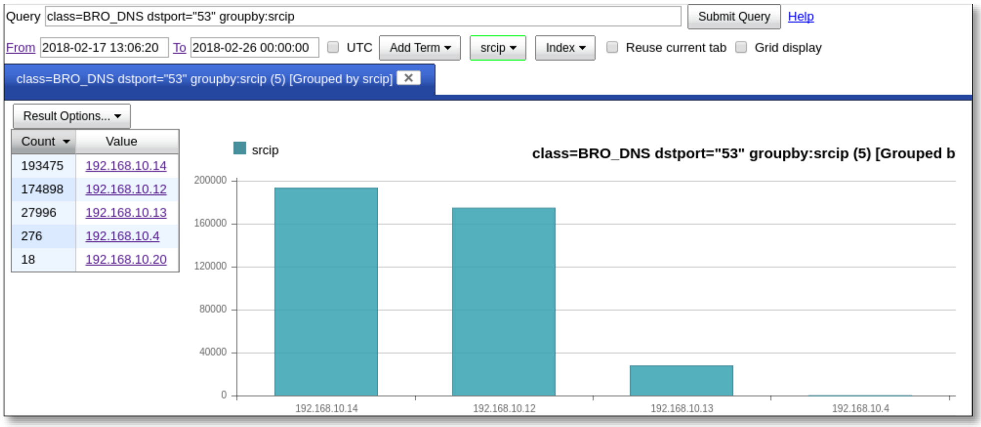
4. Internal Honeypot

As we talked in section2, Inside of our network, **Security Onion** is capturing the number of attacks which is demonstrated in Figure 7. Also we can prove it in Squert and SGUIL which are tools of Security Onion to exactly detect attackers (figure 9, 10, 11, 12). The only difference here is that we intentionally opened some ports on the firewall and when attackers pass the firewall, they face real network. Inside the firewall, as we mentioned in section2, we have 3 PCs and 4 servers for different services. By analysing captured data through Security Onion, we get different result than from section 3.



Count	Value
2166	ET SCAN SSH BruteForce Tool with fake PUTTY version
90	ET SCAN Potential SSH Scan
77	ET DROP Dshield Block Listed Source group 1
21	ET DROP Spamhaus DROP Listed Traffic Inbound group 13
18	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 56
16	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
10	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
8	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 30
8	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)
8	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 70
7	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)
5	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 78
4	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 89
4	ET INFO Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
4	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 81
4	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 86
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 72
3	ET DROP Spamhaus DROP Listed Traffic Inbound group 32
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 69
3	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 60
2	ET DROP Spamhaus DROP Listed Traffic Inbound group 7
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 55
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 93
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 66
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 24
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 84
2	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 8
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 31
2	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 80
2	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 59

Figure7: Traffic requested by users



Query class=BRO_DNS dstport="53" groupby:srcip

From 2018-02-17 13:06:20 To 2018-02-26 00:00:00 □ UTC □ Reuse current tab □ Grid display

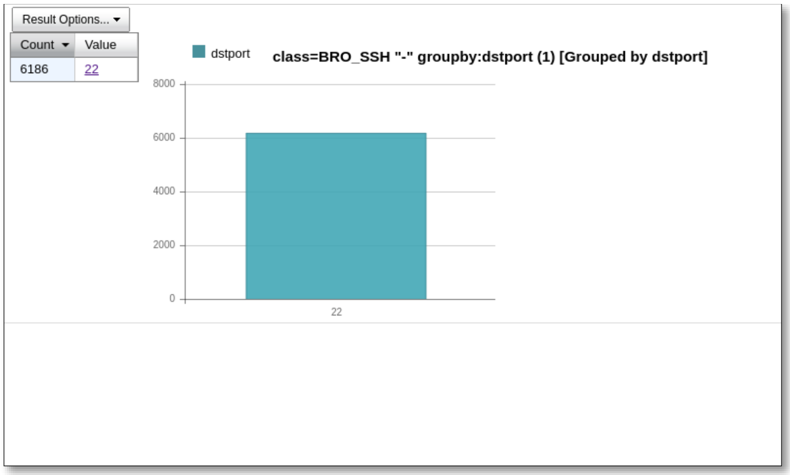
class=BRO_DNS dstport="53" groupby:srcip (5) [Grouped by srcip]

Count	Value
193475	192.168.10.14
174898	192.168.10.12
27996	192.168.10.13
276	192.168.10.4
18	192.168.10.20

class=BRO_DNS dstport="53" groupby:srcip (5) [Grouped b

Figure8: users traffic inside network

Inside network, on port 22 we had 6186 attacks which is demonstrated on Figure 9.

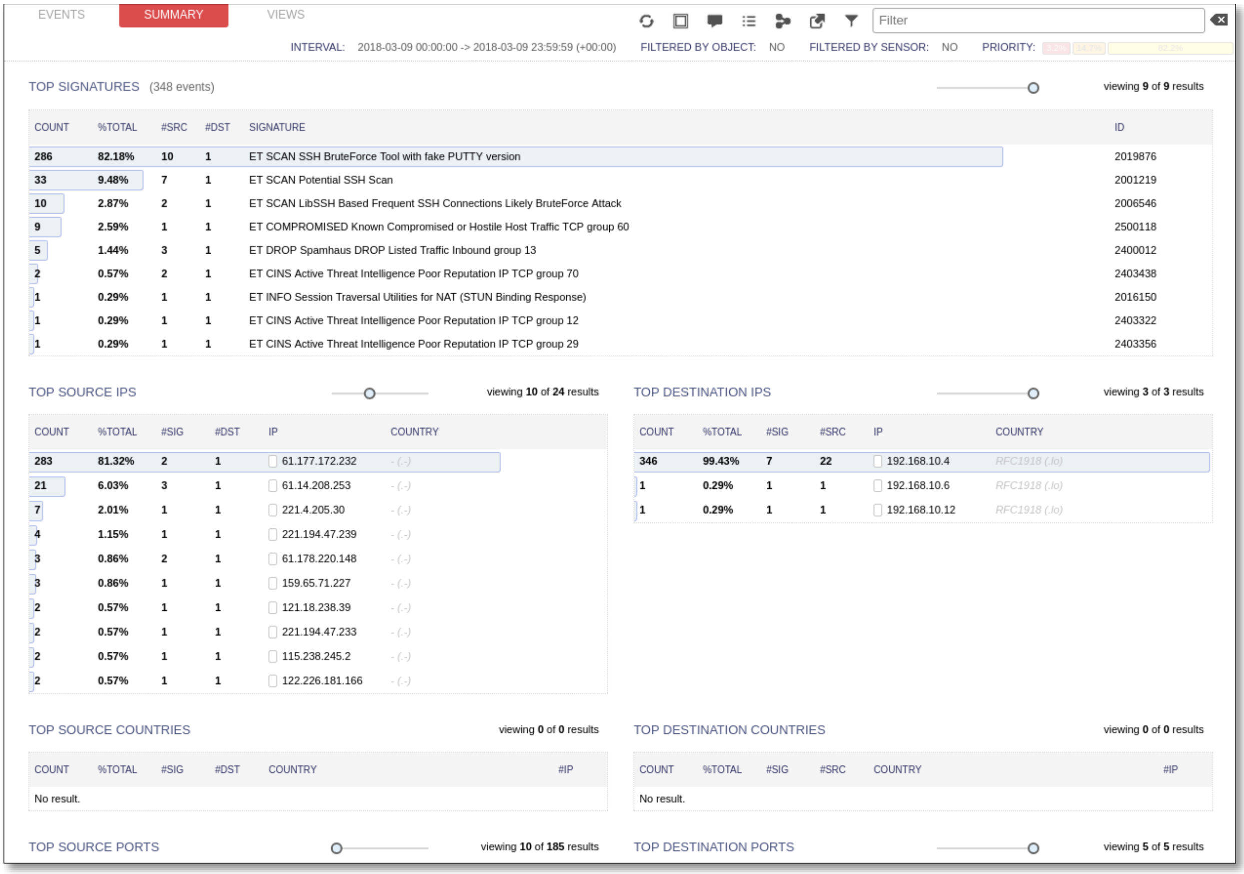


class=BRO_SSH "-" groupby:dstport (1) [Grouped by dstport]

Count	Value
6186	22

Figure9: Traffic on SSH port

As it is mentioned, we have seen 82.18% SSH BruteForce attack with fake PUTTY and other TCP protocol. We didn't see this kind of attack on the external honeypot (T-POT) (figure 10,11,12).



INTERVAL: 2018-03-09 00:00:00 -> 2018-03-09 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 3.2% 14.7% 82.2%

TOP SIGNATURES (348 events) viewing **9** of **9** results

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
286	82.18%	10	1	ET SCAN SSH BruteForce Tool with fake PUTTY version	2019876
33	9.48%	7	1	ET SCAN Potential SSH Scan	2001219
10	2.87%	2	1	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	2006546
9	2.59%	1	1	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 60	2500118
5	1.44%	3	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 13	2400012
2	0.57%	2	1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 70	2403438
1	0.29%	1	1	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	2016150
1	0.29%	1	1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 12	2403322
1	0.29%	1	1	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 29	2403356

TOP SOURCE IPS viewing **10** of **24** results

COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
283	81.32%	2	1	□ 61.177.172.232	- (.-)
21	6.03%	3	1	□ 61.14.208.253	- (.-)
7	2.01%	1	1	□ 221.4.205.30	- (.-)
4	1.15%	1	1	□ 221.194.47.239	- (.-)
3	0.86%	2	1	□ 61.178.220.148	- (.-)
3	0.86%	1	1	□ 159.65.71.227	- (.-)
2	0.57%	1	1	□ 121.18.238.39	- (.-)
2	0.57%	1	1	□ 221.194.47.233	- (.-)
2	0.57%	1	1	□ 115.238.245.2	- (.-)
2	0.57%	1	1	□ 122.226.181.166	- (.-)

TOP DESTINATION IPS viewing **3** of **3** results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
346	99.43%	7	22	□ 192.168.10.4	RFC1918 (.lo)
1	0.29%	1	1	□ 192.168.10.6	RFC1918 (.lo)
1	0.29%	1	1	□ 192.168.10.12	RFC1918 (.lo)

TOP SOURCE COUNTRIES viewing **0** of **0** results

COUNT	%TOTAL	#SIG	#DST	COUNTRY	#IP
No result.					

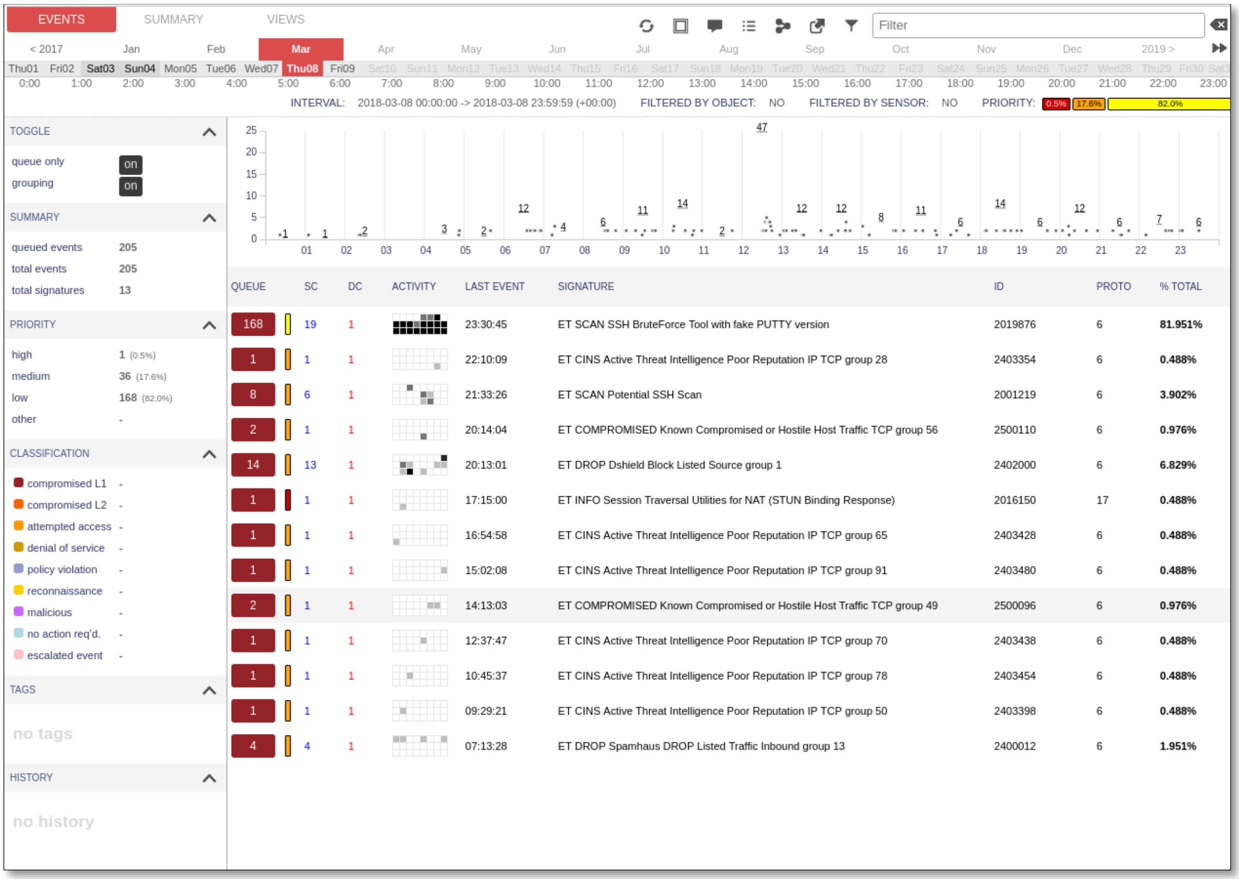
TOP DESTINATION COUNTRIES viewing **0** of **0** results

COUNT	%TOTAL	#SIG	#SRC	COUNTRY	#IP
No result.					

TOP SOURCE PORTS viewing **10** of **185** results

TOP DESTINATION PORTS viewing **5** of **5** results

Figure10: Squert summary for attacks



INTERVAL: 2018-03-08 00:00:00 -> 2018-03-08 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 0.5% 17.6% 82.0%

TOGGLE	
queue only	on
grouping	on

SUMMARY	
queued events	205
total events	205
total signatures	13

PRIORITY	
high	1 (0.5%)
medium	36 (17.6%)
low	168 (82.0%)
other	-

CLASSIFICATION	
compromised L1	-
compromised L2	-
attempted access	-
denial of service	-
policy violation	-
reconnaissance	-
malicious	-
no action req'd.	-
escalated event	-

TAGS

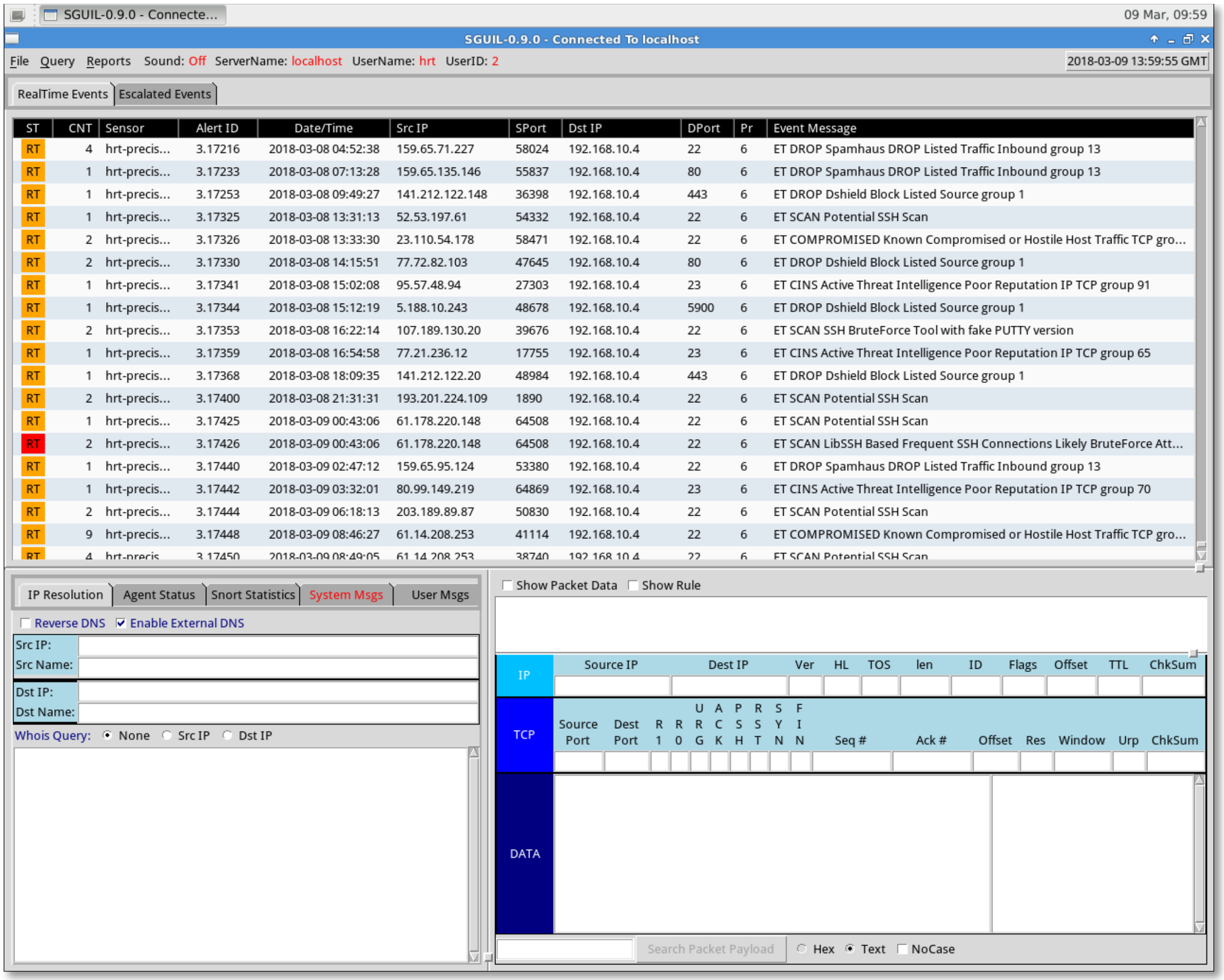
no tags

HISTORY

no history

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
168	19	1		23:30:45	ET SCAN SSH BruteForce Tool with fake PUTTY version	2019876	6	**81.951%**
1	1	1		22:10:09	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 28	2403354	6	**0.488%**
8	6	1		21:33:26	ET SCAN Potential SSH Scan	2001219	6	**3.902%**
2	1	1		20:14:04	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 56	2500110	6	**0.976%**
14	13	1		20:13:01	ET DROP Dshield Block Listed Source group 1	2402000	6	**6.829%**
1	1	1		17:15:00	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	2016150	17	**0.488%**
1	1	1		16:54:58	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 65	2403428	6	**0.488%**
1	1	1		15:02:08	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 91	2403480	6	**0.488%**
2	1	1		14:13:03	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 49	2500096	6	**0.976%**
1	1	1		12:37:47	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 70	2403438	6	**0.488%**
1	1	1		10:45:37	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 78	2403454	6	**0.488%**
1	1	1		09:29:21	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 50	2403398	6	**0.488%**
4	4	1		07:13:28	ET DROP Spamhaus DROP Listed Traffic Inbound group 13	2400012	6	**1.951%**

Figure11: Squert shows different attacks on Thurs 8th of March



SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: hrt UserID: 2 2018-03-09 13:59:55 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	hrt-precis...	3.17216	2018-03-08 04:52:38	159.65.71.227	58024	192.168.10.4	22	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 13
RT	1	hrt-precis...	3.17233	2018-03-08 07:13:28	159.65.135.146	55837	192.168.10.4	80	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 13
RT	1	hrt-precis...	3.17253	2018-03-08 09:49:27	141.212.122.148	36398	192.168.10.4	443	6	ET DROP Dshield Block Listed Source group 1
RT	1	hrt-precis...	3.17325	2018-03-08 13:31:13	52.53.197.61	54332	192.168.10.4	22	6	ET SCAN Potential SSH Scan
RT	2	hrt-precis...	3.17326	2018-03-08 13:33:30	23.110.54.178	58471	192.168.10.4	22	6	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP gro...
RT	2	hrt-precis...	3.17330	2018-03-08 14:15:51	77.72.82.103	47645	192.168.10.4	80	6	ET DROP Dshield Block Listed Source group 1
RT	1	hrt-precis...	3.17341	2018-03-08 15:02:08	95.57.48.94	27303	192.168.10.4	23	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 91
RT	1	hrt-precis...	3.17344	2018-03-08 15:12:19	5.188.10.243	48678	192.168.10.4	5900	6	ET DROP Dshield Block Listed Source group 1
RT	2	hrt-precis...	3.17353	2018-03-08 16:22:14	107.189.130.20	39676	192.168.10.4	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	1	hrt-precis...	3.17359	2018-03-08 16:54:58	77.21.236.12	17755	192.168.10.4	23	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 65
RT	1	hrt-precis...	3.17368	2018-03-08 18:09:35	141.212.122.20	48984	192.168.10.4	443	6	ET DROP Dshield Block Listed Source group 1
RT	2	hrt-precis...	3.17400	2018-03-08 21:31:31	193.201.224.109	1890	192.168.10.4	22	6	ET SCAN Potential SSH Scan
RT	1	hrt-precis...	3.17425	2018-03-09 00:43:06	61.178.220.148	64508	192.168.10.4	22	6	ET SCAN Potential SSH Scan
RT	2	hrt-precis...	3.17426	2018-03-09 00:43:06	61.178.220.148	64508	192.168.10.4	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Att...
RT	1	hrt-precis...	3.17440	2018-03-09 02:47:12	159.65.95.124	53380	192.168.10.4	22	6	ET DROP Spamhaus DROP Listed Traffic Inbound group 13
RT	1	hrt-precis...	3.17442	2018-03-09 03:32:01	80.99.149.219	64869	192.168.10.4	23	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 70
RT	2	hrt-precis...	3.17444	2018-03-09 06:18:13	203.189.89.87	50830	192.168.10.4	22	6	ET SCAN Potential SSH Scan
RT	9	hrt-precis...	3.17448	2018-03-09 08:46:27	61.14.208.253	41114	192.168.10.4	22	6	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP gro...
RT	4	hrt-precis	3.17450	2018-03-09 08:49:05	61.14.208.253	38740	192.168.10.4	22	6	ET SCAN Potential SSH Scan

□ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

□ Show Packet Data □ Show Rule

○ Hex ● Text □ NoCase

Figure12: MSSQL attack on SGUIL tools