Report(5) Captured from 17-02-2018 to 26-02-2018

1-Introduction

TThe 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. 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. 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.

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 with kind of tools which is called "Contact Form 7 Honeypot"(Figure 1).

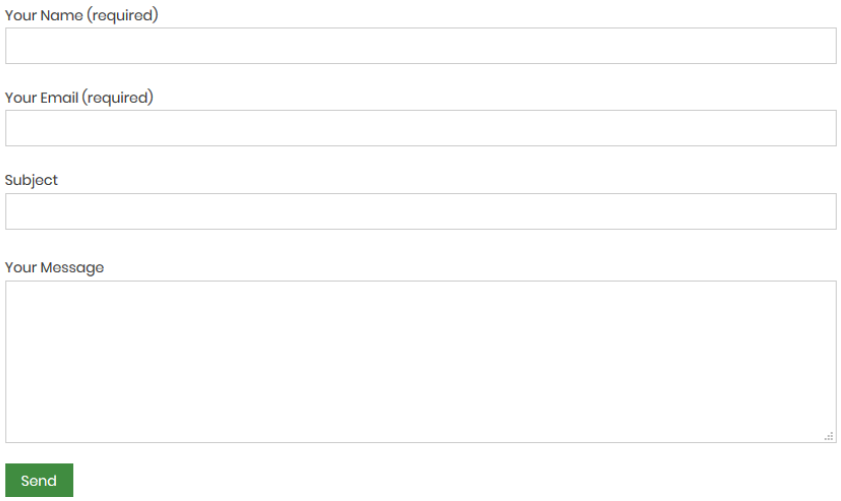

Figure1: Contact Form 7 Honeypot

Also, we use T-POT tool outside firewall 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, whose entire TCP network range as well as some important UDP services act as a honeypot, and to forward all incoming attack traffic to the best suited honeypot daemons in order to respond and process it. T-Pot includes dockerized 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. Outside firewall, there is T-POT which all user activities are capture by TAP. Inside the firewall, we have a real network with three pcs, each of which has 'like' real behaviour as they surf on the network like real users. We use benign generator to simulate this behaviour. For example one of them reacts like a secretary, the others like a manager and a IT user.

Inside servers, we have Webserver with WordPress, MySQL, Email Server (Postfix), File Server (Openmediavault), and SSH Server. We change our firewall structure to test different brands. For one month we tested Untangle firewall and now we are going to test pfSense .

Security Onion 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 many other security tools. We use Security Onion for analysing inside traffic and **Untangle** firewall for traffic of edge of network.

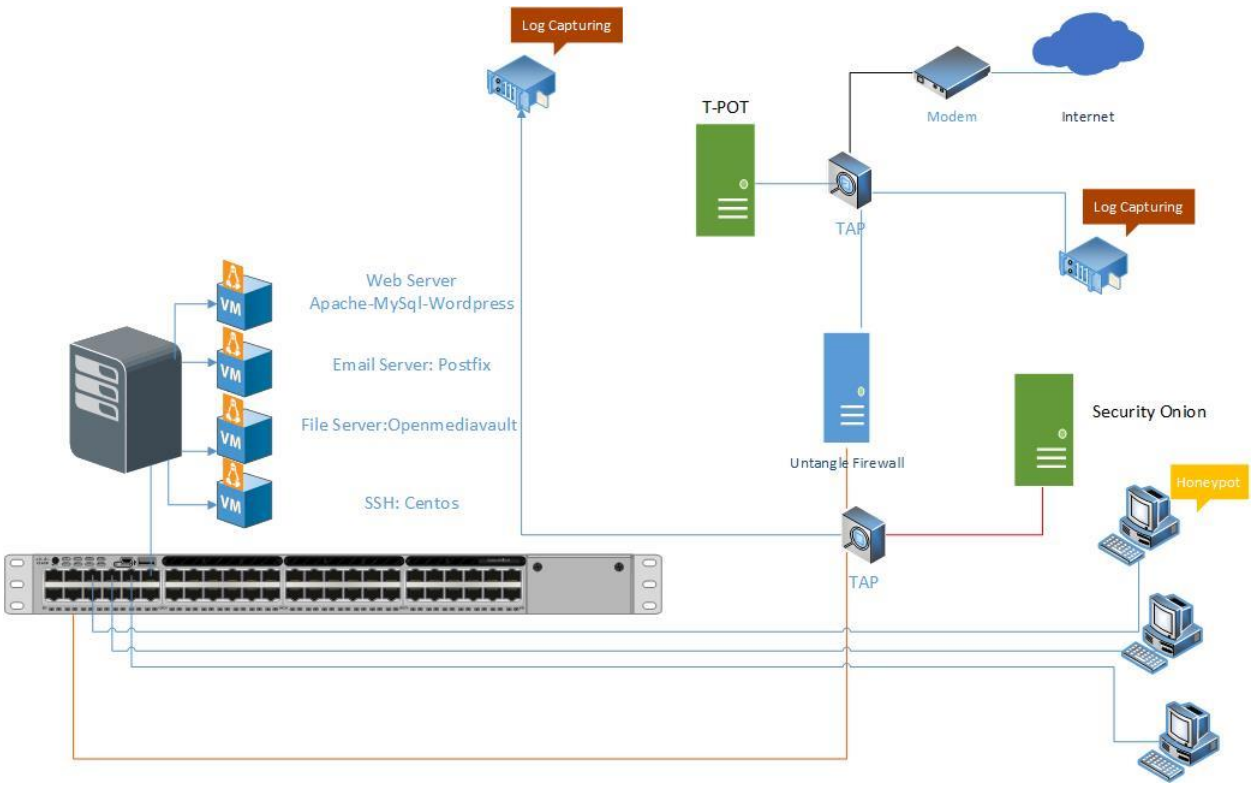

Figure2: Network Diagram

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

To simulate SSH for attackers, we use **Kippo tools** inside of firewall 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.

3- T-POT Report (Outside Firewall)

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	700558
China	133063
United States	92475
Netherlands	83823
Brazil	62705
Israel	31232
France	16966
Cyprus	10810
Turkey	10614
Japan	9879

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
61.177.172.137	67396
5.188.86.165	56764
5.188.86.207	51638
134.19.187.78	51599
5.188.87.50	51371
5.188.86.166	51157
5.188.87.51	47514
5.188.86.195	46668
5.188.86.206	44647
148.72.168.192	35438

In figure3, top 5 of countries are demonstrated by related ports. For example attacks from Russia have been 87.7% through port 2222, 8.43% through port 25, 2.83% through port 443, 0.82% through port 80 and 0.22% through port 5900.

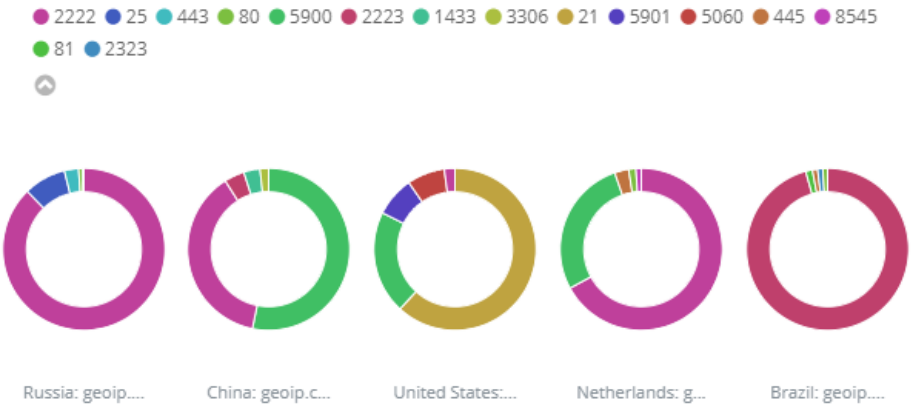

Figure3: Honeypot by country and port

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	39954
CVE-2017	15

Based on IP T-POT approximate locations of IP address which is presented on Figure 4. As it is shown in red circle, most of the attack is from Russia.

Figure4: The approximate locations of the IP addresses

Based on T-POT 81.87% of attacks are from addresses with a bad reputation, while only 18.07% are from known attackers (figure5).

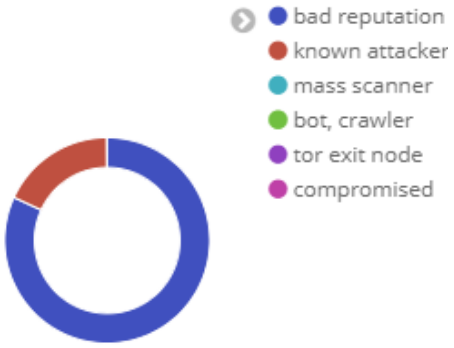

Figure5: Hoenypot source IP Reputation

In Figure 6, some attacks on NGINX is shown.

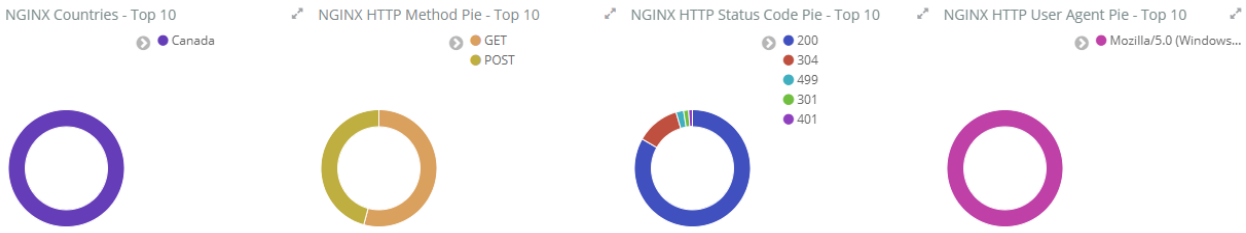

Figure6: attacks on NGINX

Around 570 of these attacks was from University of Toronto. Also we had some VNC attacks which are listed in table 4.

Table4: Top 10 Source IP of VNC attack

username	Number of occurrence
123.249.12.230	17172
107.179.25.202	11694
194.28.112.157	5651
62.4.15.196	4285
5.101.1.3	297
18.217.97.177	258
213.183.59.57	180

3.2 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:

Table5: common username used by attackers

username	Number of occurrence
root	104636
1234	78329
admin	54786
0	21155
enable	4235
shell	4209
guest	2312
	2279
supervisor	1514

user	1347

Table6: common password used by attackers

password	Number of occurrence
1234	81968
space	39747
2 space	21146
system	4235
sh	4209
admin	2965
password	2795
12345	2555
123456	2159
7ujMko0admin	1773

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.

3.3 TOP Commands

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

Table7: common command used by attackers grabbed by Cowrie

	command	Number of occurrence
1	/gweerwe323f	42
2	echo -e '\x47\x72\x6f\x70/' > //.nippon; cat //.nippon; rm -f //.nippon	42
3	cat //.nippon	42
4	rm -f //.nippon	42
5	uname -a	29

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)

Table8: common command used by attackers grabbed by Mailoney

	command	Number of occurrence
1	EHLO User	42
2	QUIT	18
3	AUTH LOGIN	14
4	STARTTLS	5

4. Inside Network

As we discussed in section2, inside of our network **Security Onion** is capturing the number of attacks. 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 open 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 and via Security Onion, we get different results than from section 3.

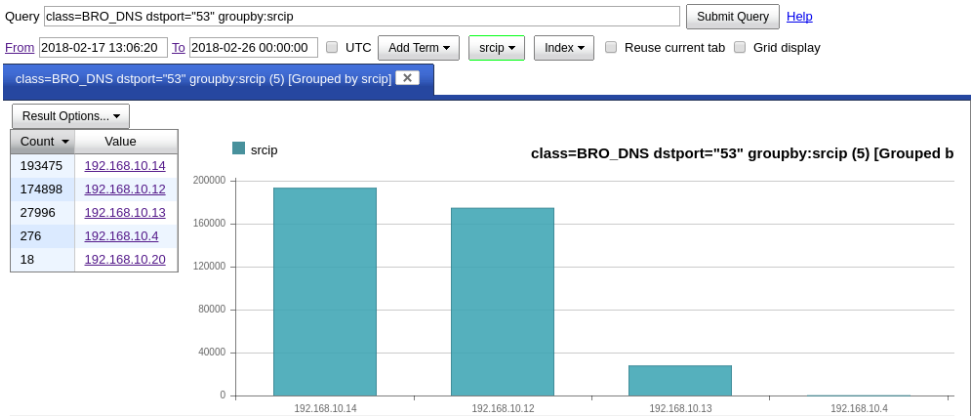

Figure7: users traffic inside network

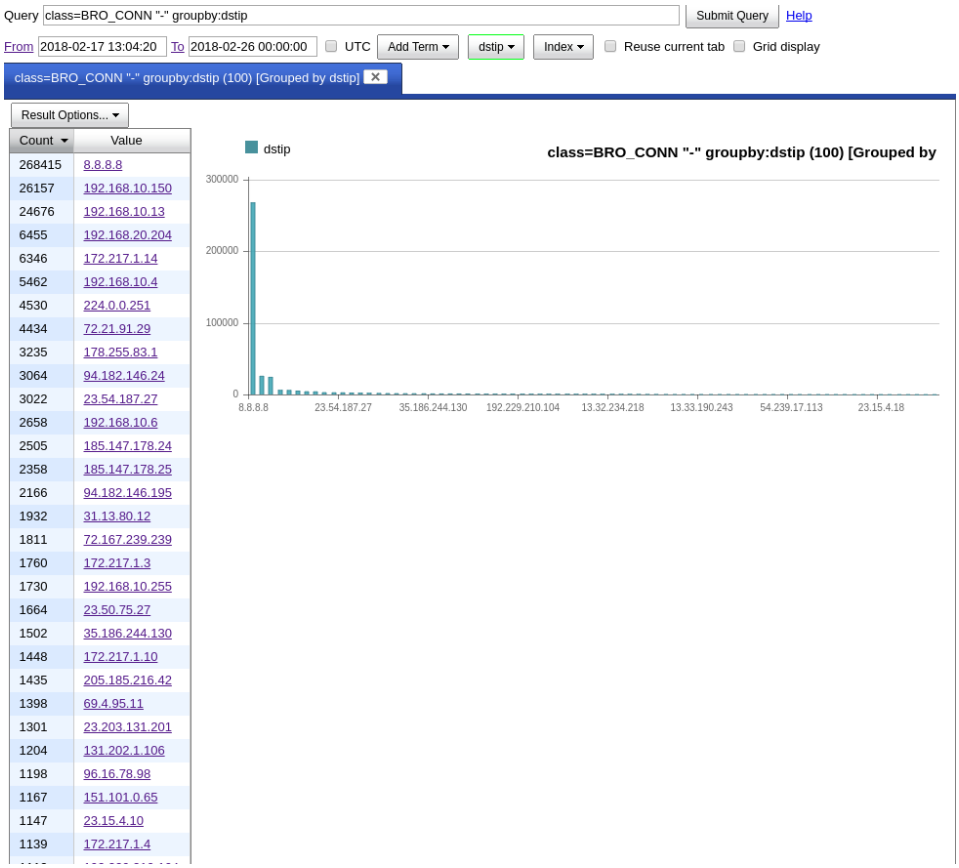

Figure8: Traffic requested by users

Inside network, on port 22 we had 3130 attacks which is demonstrated on Figure 9.

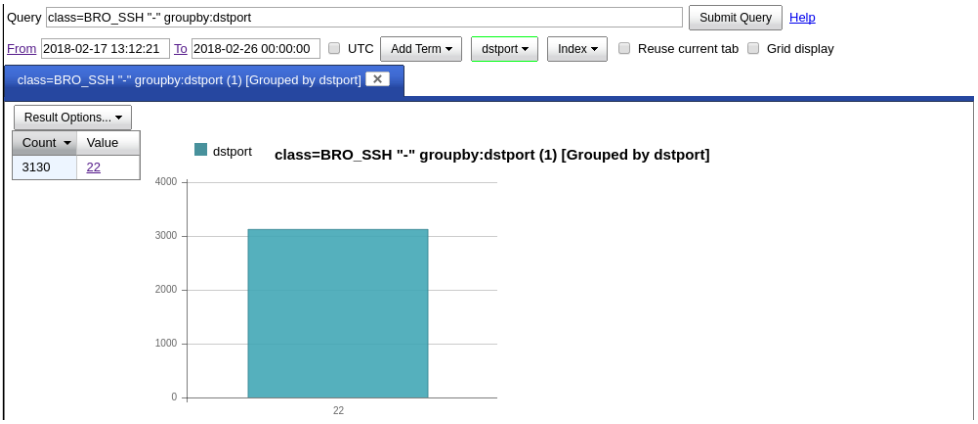

Figure9: Traffic on SSH port

As it is mentioned, we have seen new attacks on SQL, MYSQL, VNC and other protocol of TCP. We didn't see this kind of attack on T-POT(figure 10,11,12).

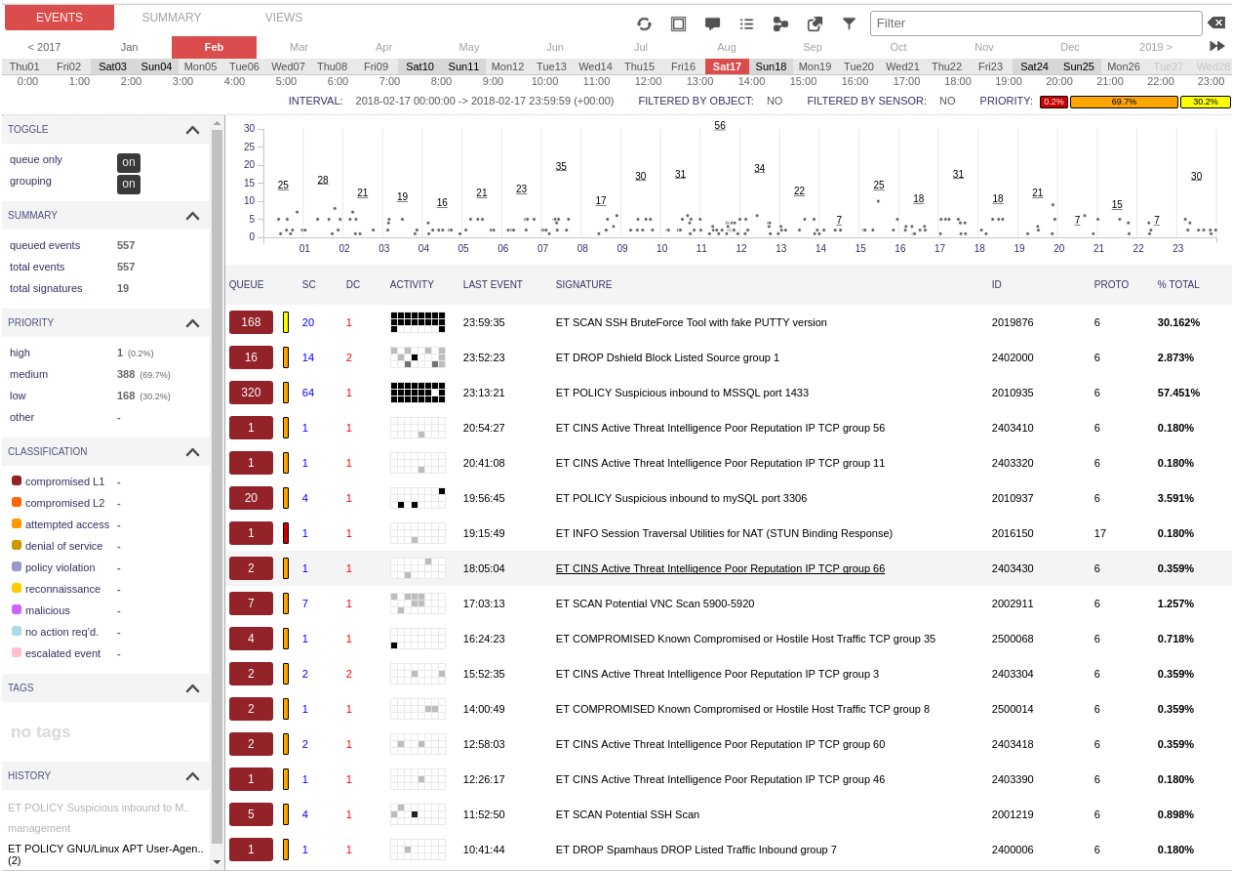

Figure10: Squert shows different attacks on Sun 17th of February

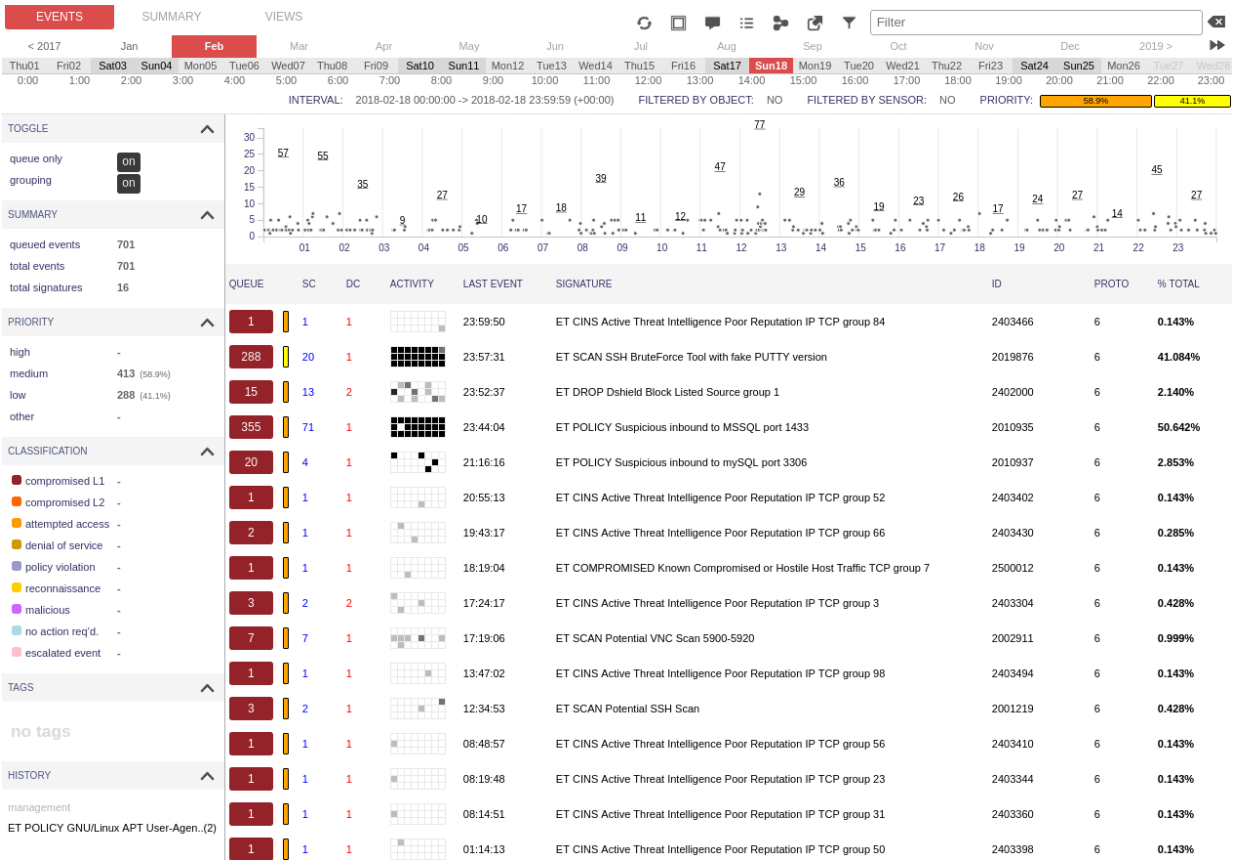

Figure11: Squert shows different attacks on Sun 18th of February

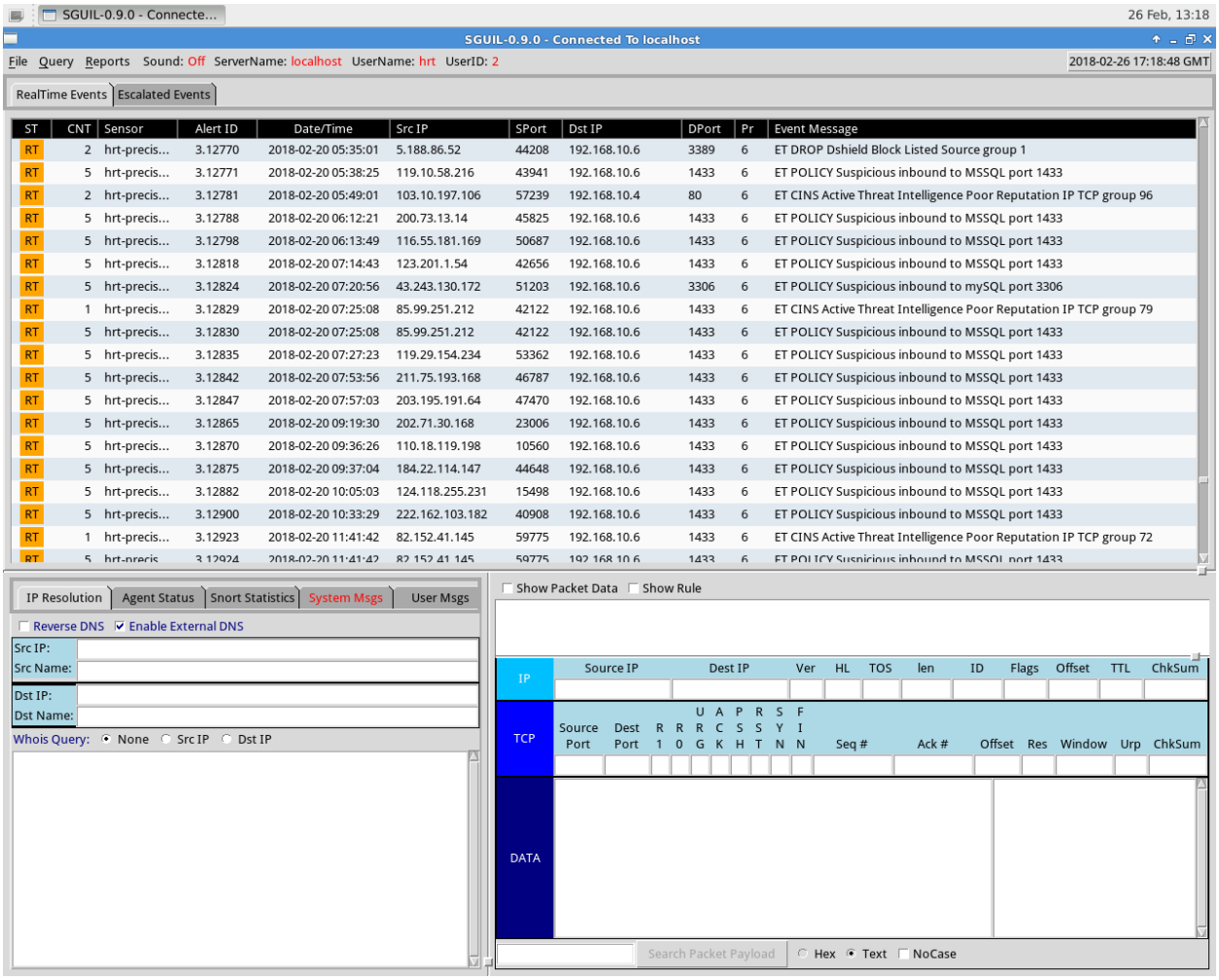

Figure12: MSSQL attack on SGUIL tools