NSM Consoles

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Learning Outcomes

- NSM Consoles
- Network Traffic
- Sguil
- Squert
- Kibana

NSM Consoles

- NSM consoles present network data in a similar format to those previously discussed; however, consoles primarily assist analysts in making decisions
- They provide an interface to manipulate and interpret multiple NSM datatypes:
  - **Full Content Data** – Network traffic stored to disk
  - **Extracted Content** – Information carved from network traffic
  - **Session Data** – A summary of conversations between hosts
  - **Transaction Data** – A more granular form of session data
  - **Statistical Data** – Characterizes network activity
  - **Metadata** – Integration of external information
  - **Alert Data** – IDS alerts that were triggered as a result of traffic

Network Traffic

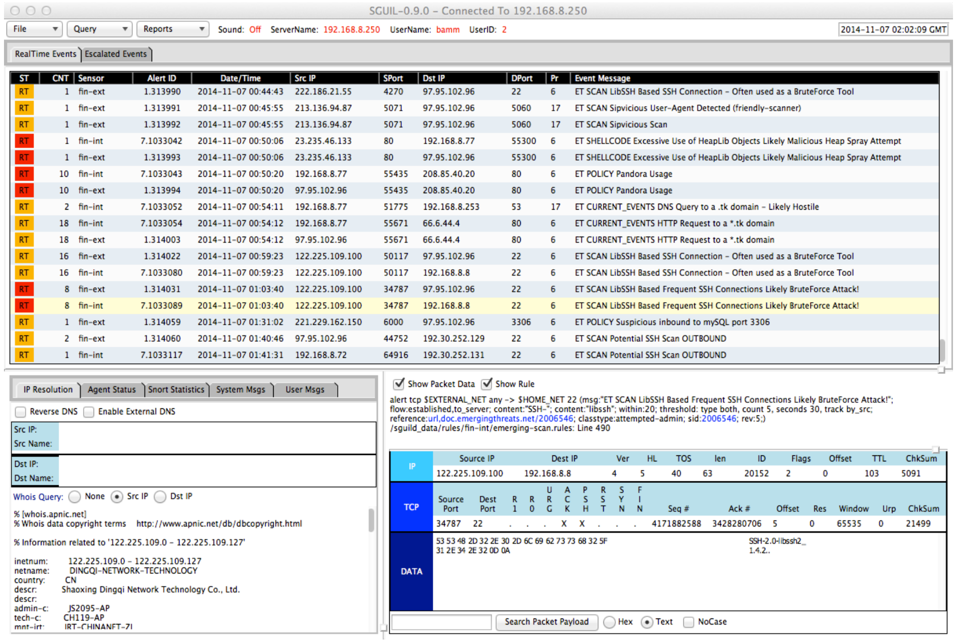
- NSM generates a lot of data, but the purpose of this data is not to have a record of network traffic
- The goal of NSM is to allow analysts determine if the event in question is benign, suspicious or malicious
- Mature CSIRTs answer this question in alignment with organizational goals, such as conducting detection and beginning response within one hour

Network Traffic

- Many tools can analyse network data, but NSM tools and consoles are designed with three goals in mind:
  - To provide analysts with an easy to use interface that is capable of displaying multiple NSM data types
  - They allow an analyst to pivot, or transition from one data type to another
  - Analysts decisions are recorded, allowing workflows to be created from the actions of multiple analysts
- Four such tools provided in Security Onion are: Sguil, Squert, Kibana and Elastic

Sguil

- Sguil is an NSM console that was first written as a proprietary application, but released to the public in 2003
- Sguil's components collect, store and present data that other tools in SO can access
- Several tools in SO utilize Sguil's SSO authentication



Sound: Off ServerName: 192.168.8.250 UserName: bamm UserID: 2

2014-11-07 02:02:09 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	fin-ext	1.313990	2014-11-07 00:44:43	222.186.21.55	4270	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	1	fin-ext	1.313991	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
RT	1	fin-ext	1.313992	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious Scan
RT	1	fin-int	7.1033042	2014-11-07 00:50:06	23.235.46.133	80	192.168.8.77	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	1	fin-ext	1.313993	2014-11-07 00:50:06	23.235.46.133	80	97.95.102.96	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	10	fin-int	7.1033043	2014-11-07 00:50:20	192.168.8.77	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	10	fin-ext	1.313994	2014-11-07 00:50:20	97.95.102.96	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	2	fin-int	7.1033052	2014-11-07 00:54:11	192.168.8.77	51775	192.168.8.253	53	17	ET CURRENT_EVENTS DNS Query to a .tk domain – Likely Hostile
RT	18	fin-int	7.1033054	2014-11-07 00:54:12	192.168.8.77	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	18	fin-ext	1.314003	2014-11-07 00:54:12	97.95.102.96	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	16	fin-ext	1.314022	2014-11-07 00:59:23	122.225.109.100	50117	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	16	fin-int	7.1033080	2014-11-07 00:59:23	122.225.109.100	50117	192.168.8.8	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	8	fin-ext	1.314031	2014-11-07 01:03:40	122.225.109.100	34787	97.95.102.96	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	8	fin-int	7.1033089	2014-11-07 01:03:40	122.225.109.100	34787	192.168.8.8	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	1	fin-ext	1.314059	2014-11-07 01:31:02	221.229.162.150	6000	97.95.102.96	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	2	fin-ext	1.314060	2014-11-07 01:40:46	97.95.102.96	44752	192.30.252.129	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	fin-int	7.1033117	2014-11-07 01:41:31	192.168.8.72	64916	192.30.252.131	22	6	ET SCAN Potential SSH Scan OUTBOUND

☐ Reverse DNS ☐ Enable External DNS

Src IP:
Src Name:

Dst IP:
Dst Name:

Whois Query: ○ None ● Src IP ○ Dst IP

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '122.225.109.0 - 122.225.109.127'

inetnum:        122.225.109.0 - 122.225.109.127
netname:        DINGQI-NETWORK-TECHNOLOGY
country:        CN
descr:          Shaoxing Dingqi Network Technology Co., Ltd.
descr:
admin-c:        JS2095-AP
tech-c:         CH119-AP
mnt-irt:        IRT-CHINANET-ZJ
```

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!";
flow:established,to_server; content:"SSH-"; content:"libssh"; within:20; threshold: type both, count 5, seconds 30, track by_src;
reference:url,doc.emergingthreats.net/2006546; classtype:attempted-admin; sid:2006546; rev:5;)
/sguild_data/rules/fin-int/emerging-scan.rules: Line 490
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	122.225.109.100	192.168.8.8	4	5	40	63	20152	2	0	103	5091

TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	34787	22	.	.	.	X	X	.	.	.	4171882588	3428280706	5	0	65535	0	21499

DATA

```
53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 32 5F      SSH-2.0-libssh2_
31 2E 34 2E 32 0D 0A                                  1.4.2..
```

○ Hex ● Text ☐ NoCase

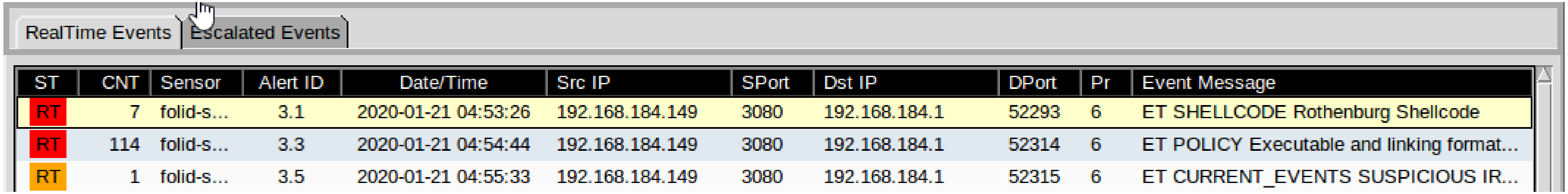
Sguil

- Sguil is a client/server application written in tcl/tk
- The server application runs on a central server, and coordinates with agents deployed on an NSM sensor
- The client is the interface the analyst uses to inspect network traffic datatypes
- Sguil is strictly a live tool, and cannot be used to analyze a network trace file

Sguil

- Key functions of Sguil:
  - Simple aggregation of similar alert data
  - Manipulating metadata and related data
  - Allows query and review of alert data
  - Perform queries and review of session data
  - Provides right-click menus to pivot to full content data, rendered as a transcript
  - Displays statistical data to count and classify events, allowing escalation and incident response

Sguil – Simple Aggregation



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	folid-s...	3.1	2020-01-21 04:53:26	192.168.184.149	3080	192.168.184.1	52293	6	ET SHELLCODE Rothenburg Shellcode
RT	114	folid-s...	3.3	2020-01-21 04:54:44	192.168.184.149	3080	192.168.184.1	52314	6	ET POLICY Executable and linking format...
RT	1	folid-s...	3.5	2020-01-21 04:55:33	192.168.184.149	3080	192.168.184.1	52315	6	ET CURRENT_EVENTS SUSPICIOUS IR...

- Sguil provides the ability to aggregate similar records into a single line of output in the console
- Grouping event together reduces the amount of noise an analyst needs to review and highlights potential attacks

Sguil – Metadata and Related Data

- Metadata provides more context about network traffic for the analyst
- Sguil allows an analyst to view basic metadata including source and destination IP addresses and hostnames (if available from DNS) for any highlighted records
- WHOIS records are also displayed for source and destination IPs
- When displaying alert data generated by SNORT or Suricata, the rule that triggered the alert is displayed, as well as the packet that triggered the alert

Sguil – Alert Data

- Sguil stores alert data in a database entity called the event table, and as such refers to alerts as event data
- Sguil incorporates four types of alert data:
  - Network IDS engines like SNORT and Suricata
    - Alerts are generated when traffic triggers an alert based on rules
    - The rules contain indicators of compromise that should be investigated if observed
    - Alert data can be found in the Event Messages column, and begin with text like ET (for Emerging Threats)

Sguil – Alert Data

- Host-based IDS engines such as Wazuh
  - Provide IDS alert data based on individual hosts
  - Requires an agent on the host machine
- Event data from non-IDS sources
  - Sguil collects data created by the Passive Real-Time Asset Detection System (PRADS)
- Transaction data generated by Zeek (formerly Bro)
  - Records Uniform Resource Locators (URLs)
  - Displayed with the preface URL

Sguil – Session Data

- Sguil refers to session data as SANCP data
- The Security Analyst Network Connection Profiler (SANCP) is a tool written by John Curry that was packaged with early versions of Sguil.
- SANCP has been replaced with PRADS in later versions
- As well as generating session data, PRADS collects network device information in the form of device profiles
- Like full content data, session data is always written to disk, regardless of the context of the information (if it is deemed suspicious)

Sguil – Session Data

- Session data is not displayed by default, analysts run queries against the SANCP table to retrieve it
- A more common workflow is to pivot from alert data to session data, using a point of interest to perform the query
- Session data queries allow URL based data to be further investigated using a right-click action

Sguil – Full Content Data

- Just as Sguil allows pivoting to session data, it can also pivot to full content data
- When displaying full content data, it is often useful to display this data as a transcript for known protocols
- The transcript is similar to the output displayed in Wireshark when viewing a TCP stream
- Full content data is a reconstruction of data saved to the disk by Netsniff-ng

Sguil – Alert Data

- Sguil was designed as a real-time console for analysts sitting in a Security Operations Centre (SOC)
- Sguil is not an alert browser and should not be treated as an alert log
- Analysts should monitor and investigate Sguil alerts as they appear, determining if they are benign, suspicious or malicious, and assign a label to the alert
- This will change the status of the event from Real-Time (RT), to the classification chosen by the analyst

Sguil – Alert Data

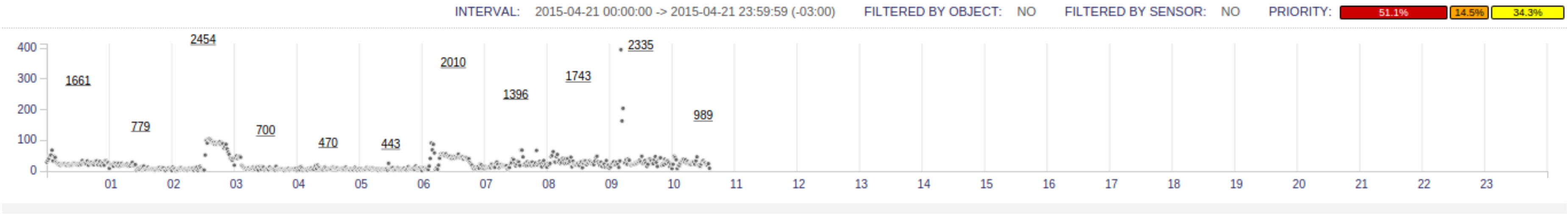
- Sguil includes the following default categories:
    - Category I Unauthorized Root/Admin Access
    - Category II Unauthorized User Access
    - Category III Attempted Unauthorized Access
    - Category IV Successful Denial of Service Attack
    - Category V Poor Security Practice or Policy Violation
    - Category VI Reconnaissance/Probes/Scans
    - Category VII Virus Infection
- The event categories are mapped to the function keys F1-F7
- F8 classifies an event as being of no consequence

Sguil – Alert Data

- Once an event has been classified, it will disappear from the Real-Time display, as the event has been “handled”, but it will remain in the database
- Pressing F9 on an event, escalates the event for processing by a senior analyst

Squert

- Squert is an open source interface for NSM data
- Squert provides access to the Sguil database using a web browser
- The Squert client presents key elements of different datatypes as record in rows
- Squert allows for visualization and supporting information to events in the Sguil database
- Squert includes a graph of events grouped over time



INTERVAL: 2015-04-21 00:00:00 -> 2015-04-21 23:59:59 (-03:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 51.1% 14.5% 34.3%

Kibana

- Kibana replaced Snorby as a web interface and provides advanced analytics for NSM data
- Kibana can create custom dashboards and graphs, but also provide point and click access to alert information, transaction data, statistics, metadata, and session records
- Kibana integrates the functions of ElasticSearch as can query normalized records from any sensor

Summary

- NSM consoles display captured records to allow analysts to make informed decisions about network events
- The goal of NSM is to allow analysts determine if the event discovered in the network traffic is benign, suspicious or malicious
- Sguil is a thick-client that analysts use to inspect network traffic datatypes
- Squert is a web-based NSM console that provides visualization and supporting information
- Kibana provides dashboards to summarize data, but also has access to many data types and provides point and click access

References

- Bejtlich, R. (2013). Chapter 8: NSM Consoles. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Kibana. (n.d.). Retrieved March 22, 2020, from https://securityonion.readthedocs.io/en/latest/kibana.html
- Visscher, B., & Viklund, A. (n.d.). Sguil: The Analyst Console for Network Security Monitoring. Retrieved March 22, 2020, from http://bammv.github.io/sguil/screenshots.html
- the squertproject. (n.d.). Retrieved March 22, 2020, from http://www.squertproject.org/