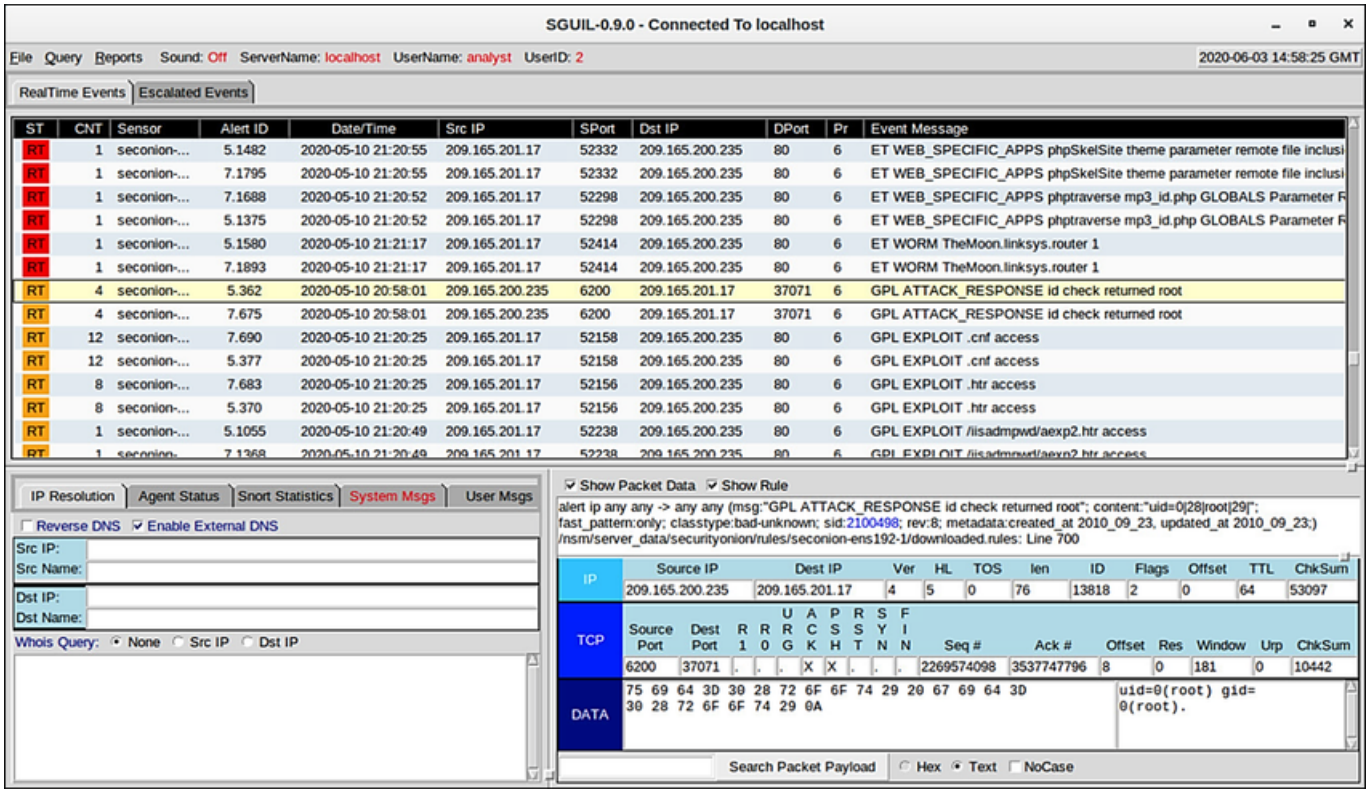
Alert data consists of messages generated by intrusion prevention systems (IPSs) or intrusion detection systems (IDSs) in response to traffic that violates a rule or matches the signature of a known exploit. A network IDS (NIDS), such as Snort, comes configured with rules for known exploits.
Alerts are generated by Snort and are made readable and searchable by the Sguil and Squert applications, which are part of the Security Onion suite of NSM tools. In this article, I will be talking about security data in cybersecurity.

A testing site that is used to determine if Snort is operating is the tesmyids site. Search for it on the internet. It consists of a single webpage that displays only the following text **uid=0(root) gid=0(root) groups=0(root)**. If Snort is operating correctly and a host visits this site, a signature will be matched and an alert will be triggered. This is an easy and harmless way to verify that the NIDS is running.
The Snort rule that is triggered is:

```
alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check
returned root"; content:"uid=0|28|root|29|"; fast\_pattern:only;
classtype:bad-unknown; sid:2100498; rev:8;)
```

This rule generates an alert if **any IP address** in the network receives data from an external source that contains content with text matching the pattern of **uid=0(root)**. The alert contains the message **GPL ATTACK_RESPONSE id check returned root**. The ID of the Snort rule that was triggered is **2100498**.
The highlighted line in the figure displays a Sguil alert that was generated by visiting the testmyids website. The Snort rule and the packet data for the content received from the testmyvids webpage is displayed in the lower right-hand area of the Sguil interface.

Sguil Console Showing Test Alert from Snort IDS



Session and Transaction Data

Session data is a record of a conversation between two network endpoints, which are often a client and a server. The server could be inside the enterprise network or at a location accessed over the internet. Session data is data about the session, not the data retrieved and used by the client.
Session data will include identifying information such as **the five tuples** of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use. Data about the session typically includes a session ID, the amount of data transferred by source and destination, and information related to the duration of the session. Zeek, formerly Bro, is a network security monitoring tool you will use in labs later in the course. .

Zeek Session Data – Partial Contents

12345678910111213

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567	CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	5	4
1320279567	CI6Ueb3SkSJHwASNN4	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.56194	905	731	9	8
1320279567	CaTMSv1Sb8HtFunqjj	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	15	13

1. **ts**: session start timestamp
2. **uid**: unique session ID
3. **id.orig_h**: IP address of host that originated the session (source address)
4. i**d.orig_p**: protocol port for the originating host (source port)
5. **id.resp_h**: IP address of host responding to the originating host (destination address)
6. **id.resp_p**: protocol of responding host (destination port)
7. **proto**: transport layer protocol for session
8. **service**: application layer protocol
9. **duration**: duration of the session
10. **orig_bytes**: bytes from originating host
11. **resp_bytes**: bytes from responding host
12. **orig_packets**: packets from the originating host
13. **resp_packets**: packets from responding host

Transaction data consists of the messages that are exchanged during network sessions. These transactions can be viewed in packet capture transcripts.
Device logs kept by servers also contain information about the transactions that occur between clients and servers.
For example, a session might include the downloading of content from a web server, as shown in the figure.
The transactions that represent the requests and replies would be logged in an access log on the server or by a NIDS like Zeek. The session is all traffic involved in making up the request, the transaction is the request itself.

Transaction Data

GET /home/index.html HTTP/1.1Host: www.example.comContent-Type: text/plain Tractor-Encoding: chunkedMozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0HTTP/1.1 200 OK Date: Fri, 10 Oct 2015 23:59:59 GMT Content-Type: text/plain<text returned>192.168.1.10 – anyUser [10/Oct/2015:13:55:36 -0500] “GET /index.html HTTP/1.1” 200 326
Transaction data record as a web server access log entry.

Full Packet Captures

Full packet captures are the most detailed network data that is generally collected. Because

of the amount of detail, they are also the most storage and retrieval intensive types of data used in NSM. Full packet captures contain not only data about network conversations, like session data.
Full packet captures also contain the actual contents of the conversations. Full packet captures contain the text of email messages, the HTML in webpages, and the files that enter or leave the network. Extracted content can be recovered from full packet captures and analyzed for malware or user behaviour that violates business and security policies.
The familiar tool Wireshark is very popular for viewing full packet captures and accessing the data associated with network conversations.
The figure illustrates the interface for the Network Analysis Monitor component of the Cisco Prime Infrastructure system, which, like Wireshark, can display full packet captures.

Cisco Prime Network Analysis Module – Full Packet Captur

Statistical Data

Like session data, statistical data is about network traffic. Statistical data is created through the analysis of other forms of network data. Conclusions can be made that describe or predict network behaviour from this analysis. Statistical characteristics of normal network behaviour can be compared to current network traffic in an effort to detect anomalies.

Statistics can be used to characterize normal amounts of variation in network traffic patterns in order to identify network conditions that are significantly outside of those ranges. Statistically, significant differences should raise alarms and prompt investigation.

Network Behavior Analysis (NBA) and Network Behavior Anomaly Detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyze NetFlow or Internet Protocol Flow Information Export (IPFIX) network telemetry data. Techniques such as predictive analytics and artificial intelligence perform advanced analyses of detailed session data to detect potential security incidents.

Note: IPFIX is the IETF standard version of Cisco NetFlow version 9.
An example of an NSM tool that utilizes statistical analysis is Cisco Cognitive Threat Analytics.

It is able to find a malicious activity that has bypassed security controls or entered the network through unmonitored channels (including removable media) and is operating inside an organization’s environment.

Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modelling of networks. It creates a baseline of the traffic in a network and identifies anomalies.
It analyzes user and device behaviour, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in the infrastructure.
The figure illustrates an architecture for Cisco Cognitive Threat Analytics.

The figure shows three internal users with each icon having an arrow pointing to the behavioural analysis icon.
Another set of three arrows goes from the behavioural analysis icon to the potential threat icon to the right. Below behavioural analysis are two more icons: anomaly detection and machine learning.
An arrow goes from behavioural analysis to anomaly detection, from anomaly detection to machine learning, and from machine learning pointing to behavioural analysis.

Action Point

Get My 66 Page eBook on How to Run Success Ads ON TikTok for 2,000 Naira. Click Here to Buy.

https://spoo.me/iy8taz

Get my 90 Page ebook on How to Run Ads on Facebook. Click here to buy now.

PS: Are you a Nigerian resident abroad and you need to send money to your loved ones back home? The stress is over now! Send money to Nigeria using the MonieWorld app. It's fast, easy and has great rates! MonieWorld is powered by Moniepoint. Sign up with my link

https://spoo.me/iy8taz

P.S.: If you need private online training on any of the ICT courses I offer here and you are in Nigeria, please send me a DM on my WhatsApp at **+2348103180831.** Please note that the Training will be 100percent online. It will be delivered via Zoom or Google Meet.

PS: I know you might agree with some of the points raised in this article or disagree with some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

PEOPLE ALSO READ: The 10x Employee. Building Leaders in Our Organisations

Related posts:

1. Cyber Killer Chain In Cybersecurity: Facts To Know
2. The 10x Whatsapp Group Administrator . Being a Leader With a Difference
3. The 10x Employee. Building Leaders in Our Organisations
4. Building a 10x Career. The Untaken Path to Career Growth