Deployment of a Security operation Analyst(SOC) ANALYST Lab : SIEM and IDS/IPS Solutions

Cyber Security Enterprise Tools :-

1. **Snort IDS**
2. **Wazuh SIEM**
3. **Splunk Enterprise Security**

Machines used for setting up the Network

1. **Parrot OS :- as a Host Machine for Splunk and Snort**
2. **Kalilinux OS :- as a Host Machine for Wazuh**
3. **Admin :- Wazuh Agent**
4. **Windows OS :- Wazuh Agent 1**
5. **Metasploitable Machine :- Target Machine for the Snort IDS**

Intrusion Detection System (IDS)

IDS is a passive monitoring solution for detecting possible malicious activities/patterns, abnormal incidents, and policy violations. It is responsible for generating alerts for each suspicious event.

There are two main types of IDS systems;

Network Intrusion Detection System (NIDS) - NIDS monitors the traffic flow from various areas of the network. The aim is to investigate the traffic on the entire subnet. If a signature is identified, an alert is created.
Host-based Intrusion Detection System (HIDS) - HIDS monitors the traffic flow from a single endpoint device The aim is to investigate the traffic on a particular device. If a signature is identified, an alert is created.

Intrusion Prevention System (IPS)

IPS is an active protecting solution for preventing possible malicious activities/patterns, abnormal incidents, and policy violations. It is responsible for stopping/preventing/terminating the suspicious event as soon as the detection is performed. There are four main types of IPS systems:

1.Network Intrusion Prevention System (NIPS) - NIPS monitors the traffic flow from various areas of the network. The aim is to protect the traffic on the entire subnet. If a signature is identified, the connection is terminated.

2.Behaviour-based Intrusion Prevention System (Network Behaviour Analysis - NBA) - Behaviour-based systems monitor the traffic flow from various areas of the network. The aim is to protect the traffic on the entire subnet. If a signature is identified, the connection is terminated.Network Behaviour Analysis System works similar to NIPS. The difference between NIPS and Behaviour-based is; behaviour based systems require a training period (also known as "baselining") to learn the normal traffic and differentiate the malicious traffic and threats. This model provides more efficient results against new threats.

The system is trained to know the "normal" to detect "abnormal". The training period is crucial to avoid any false positives. In case of any security breach during the training period, the results will be highly problematic. Another critical point is to ensure that the system is well trained to recognise benign activities.

3.Wireless Intrusion Prevention System (WIPS) - WIPS monitors the traffic flow from of wireless network. The aim is to protect the wireless traffic and stop possible attacks launched from there. If a signature is identified, the connection is terminated.

4.Host-based Intrusion Prevention System (HIPS) - HIPS actively protects the traffic flow from a single endpoint device. The aim is to investigate the traffic on a particular device. If a signature is identified, the connection is terminated.

Detection/Prevention Techniques

There are three main detection and prevention techniques used in IDS and IPS solutions;

Technique Approach
Signature-Based

This technique relies on rules that identify the specific patterns of the known malicious behaviour. This model helps detect known threats.
Behaviour-Based

This technique identifies new threats with new patterns that pass through signatures. The model compares the known/normal with unknown/abnormal behaviours. This model helps detect previously unknown or new threats.
Policy-Based This technique compares detected activities with system configuration and security policies. This model helps detect policy violations.

SNORT is an open-source, rule-based Network Intrusion Detection and Prevention System (NIDS/NIPS). It was developed and still maintained by Martin Roesch, open-source contributors, and the Cisco Talos team.

Capabilities of Snort:-
Live traffic analysis
Attack and probe detection
Packet logging
Protocol analysis
Real-time alerting
Modules & plugins
Pre-processors
Cross-platform support! (Linux & Windows)
Snort has three main use models;

Sniffer Mode - Read IP packets and prompt them in the console application.
Packet Logger Mode - Log all IP packets (inbound and outbound) that visit the network.
NIDS (Network Intrusion Detection System) and NIPS (Network Intrusion Prevention System) Modes - Log/drop the packets that are deemed as malicious according to the user-defined rules.

For Snort to check and test the configuration file the commands are respectively:-

```
$sudo snort -c /etc/snort/snort.conf
$sudo snort -c /etc/snort/snort.conf  -T #(snort.conf file is the configuration file)
```

Parameter	Description
-V --version	This parameter provides information about your instance version.
-c	Identifying the configuration file
-T	Snort's self-test parameter, you can test your setup with this parameter.
-q	Quiet mode prevents snort from displaying the default banner and initial information about your setup

we can read the file using the -r parameter
for ex:- $sudo snort -r logname.log
More Examples:-
sudo snort -r logname.log -X
sudo snort -r logname.log icmp
sudo snort -r logname.log tcp
sudo snort -r logname.log 'udp and port 53'

NIDS mode parameters are explained in the table below;

Parameter Description

-c Defining the configuration file.

-T Testing the configuration file.

-N Disable logging.

-D Background mode.

-A Alert modes;

full: Full alert mode, providing all possible information about the alert. This one also is the default mode; once you use -A and don't specify any mode, snort uses this mode.

fast: Fast mode shows the alert message, timestamp, source and destination IP, along with port numbers.

console: Provides fast style alerts on the console screen.

cmg: CMG style, basic header details with payload in hex and text format.

none: Disabling alerting.

IPS mode and dropping packets

Snort IPS mode activated with -Q --daq afpacket parameters. You can also activate this mode by editing snort.conf file. However, you don't need to edit snort.conf file in the scope of this room. Review the bonus task or snort manual for further information on daq and advanced configuration settings: -Q --daq afpacket

Capabilities of Snort are not limited to sniffing, logging and detecting/preventing the threats. PCAP read/investigate mode helps you work with pcap files. Once you have a pcap file and process it with Snort, you will receive default traffic statistics with alerts depending on your ruleset.

Reading a pcap without using any additional parameters we discussed before will only overview the packets and provide statistics about the file. In most cases, this is not very handy. We are investigating the pcap with Snort to benefit from the rules and speed up our investigation process by using the known patterns of threats.

PCAP mode parameters are explained in the table below;

Parameter	Description
-r / --pcap-single=	Read a single pcap
--pcap-list=""	Read pcaps provided in command (space separated).
--pcap-show	Show pcap name on console during processing.

Rules cannot be processed without a header. Rule options are "optional" parts. However, it is almost impossible to detect sophisticated attacks without using the rule options.

Action

There are several actions for rules. Make sure you understand the functionality and test it before creating rules for live systems. The most common actions are listed below.

- alert: Generate an alert and log the packet.
- log: Log the packet.
- drop: Block and log the packet.
- reject: Block the packet, log it and terminate the packet session.

Protocol

Protocol parameter identifies the type of the protocol that filtered for the rule.

Note that Snort2 supports only four protocols filters in the rules (IP, TCP, UDP and ICMP). However, you can detect the application flows using port numbers and options. For instance, if you want to detect FTP traffic, you cannot use the FTP keyword in the protocol field but filter the FTP traffic by investigating TCP traffic on port 21.

General Rule Options

Msg The message field is a basic prompt and quick identifier of the rule. Once the rule is triggered, the message filed will appear in the console or log. Usually, the message part is a one-liner that summarises the event.

Sid

Snort rule IDs (SID) come with a pre-defined scope, and each rule must have a SID in a proper format. There are three different scopes for SIDs shown below.

<100: Reserved rules

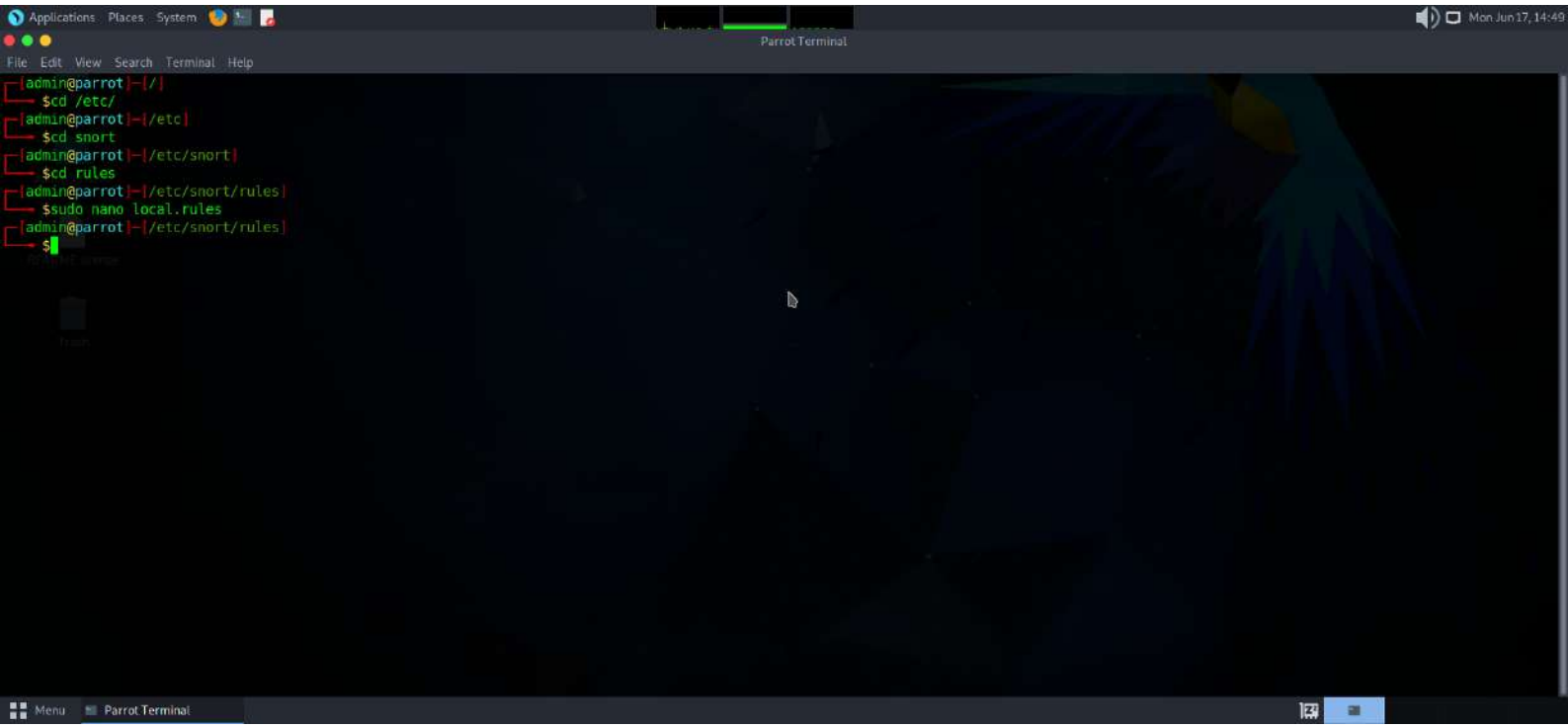
100-999,999: Rules came with the build.

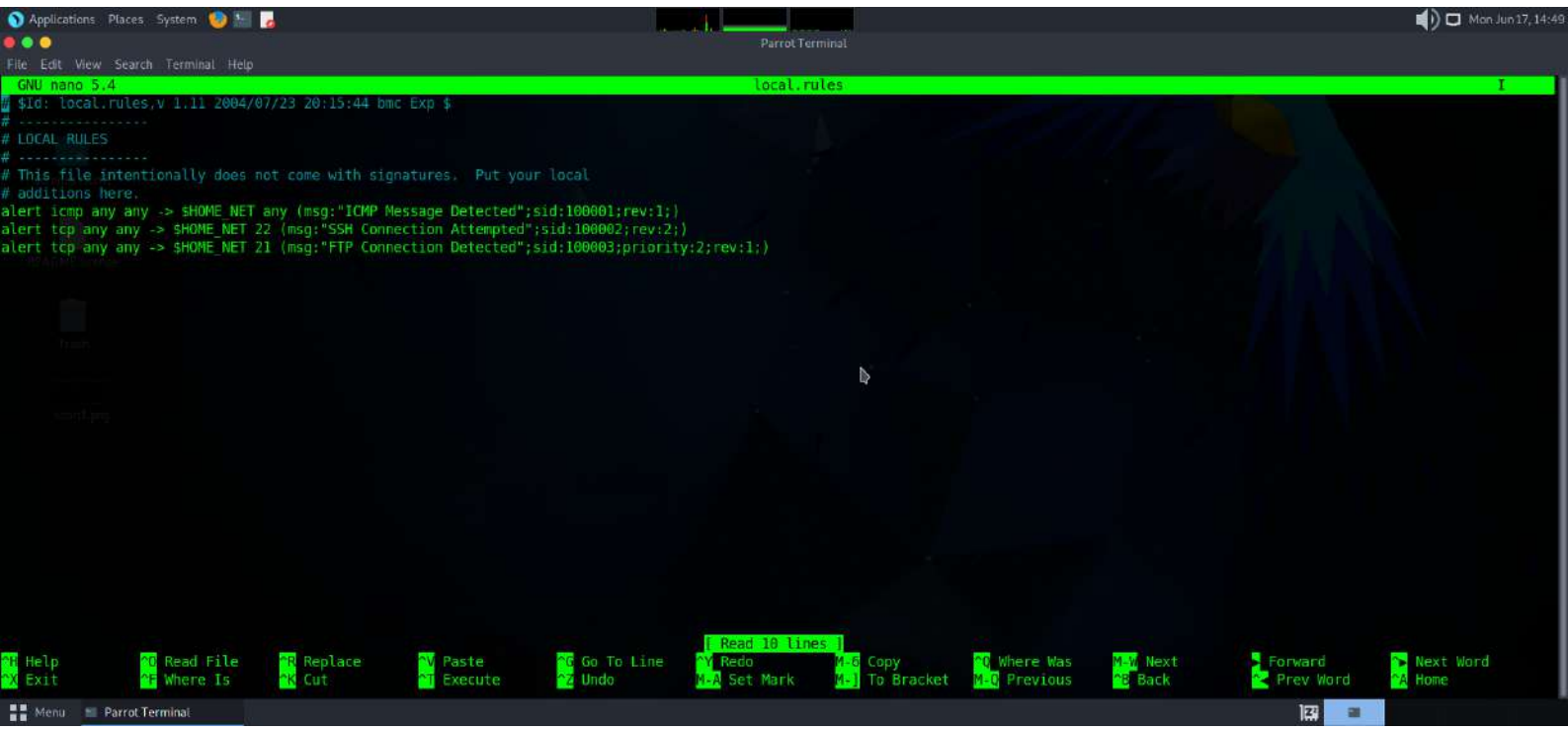
>=1,000,000: Rules created by user.

Each rule can have additional information or reference to explain the purpose of the rule or threat pattern. That could be a Common Vulnerabilities and Exposures (CVE) id or external information. Having references for the rules will always help analysts during the alert and incident investigation.

Rev

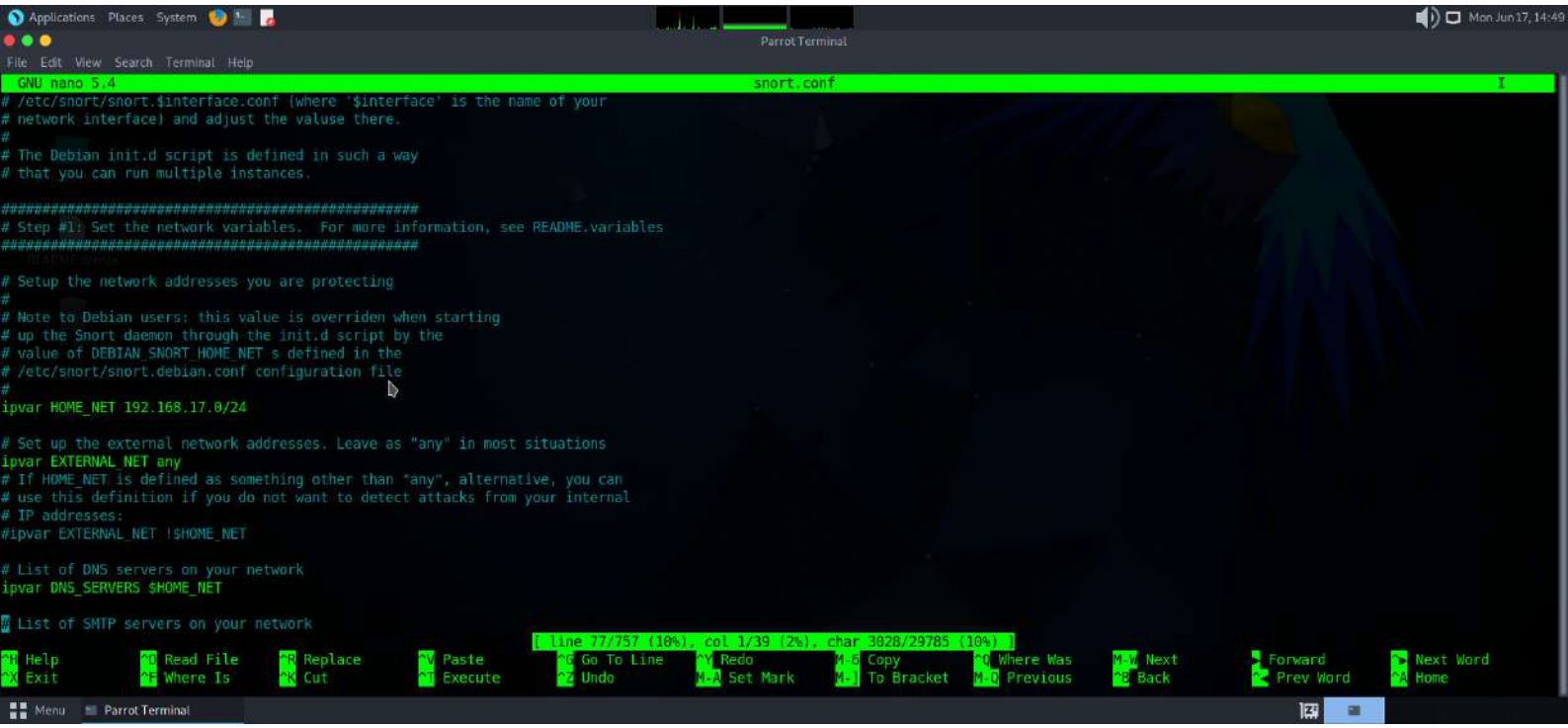
Snort rules can be modified and updated for performance and efficiency issues. Rev option help analysts to have the revision information of each rule. Therefore, it will be easy to understand rule improvements. Each rule has its unique rev number, and there is no auto-backup feature on the rule history. Analysts should keep the rule history themselves. Rev option is only an indicator of how many times the rule had revisions.

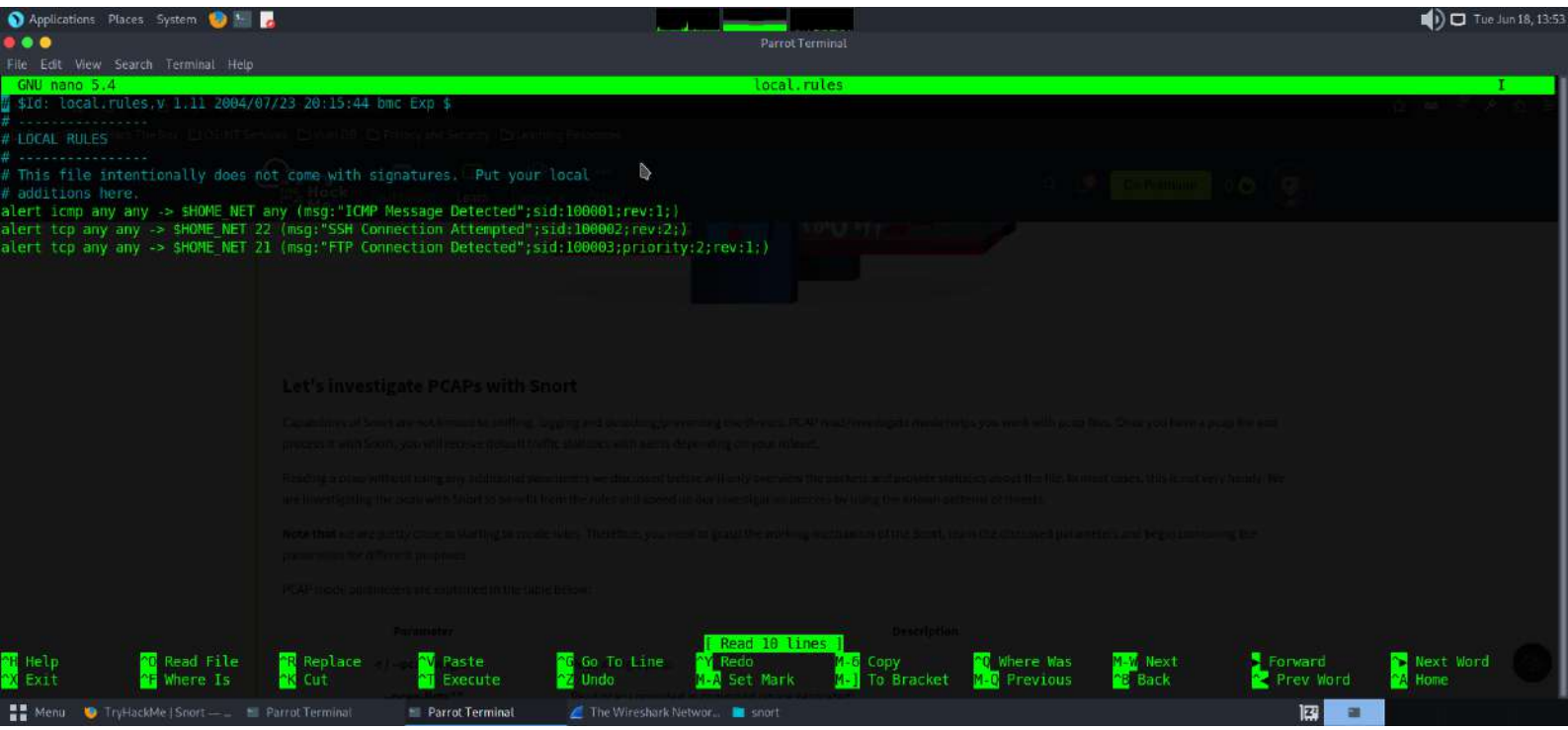

Applications Places System
Mon Jun 17, 14:49
Parrot Terminal
File Edit View Search Terminal Help
[admin@parrot]-[/]
$cd /etc/
[admin@parrot]-[/etc]
$cd snort
[admin@parrot]-[/etc/snort]
$cd rules
[admin@parrot]-[/etc/snort/rules]
$sudo nano local.rules
[admin@parrot]-[/etc/snort/rules]
$
Menu
Parrot Terminal


Applications Places System
Mon Jun 17, 14:49
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4 local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

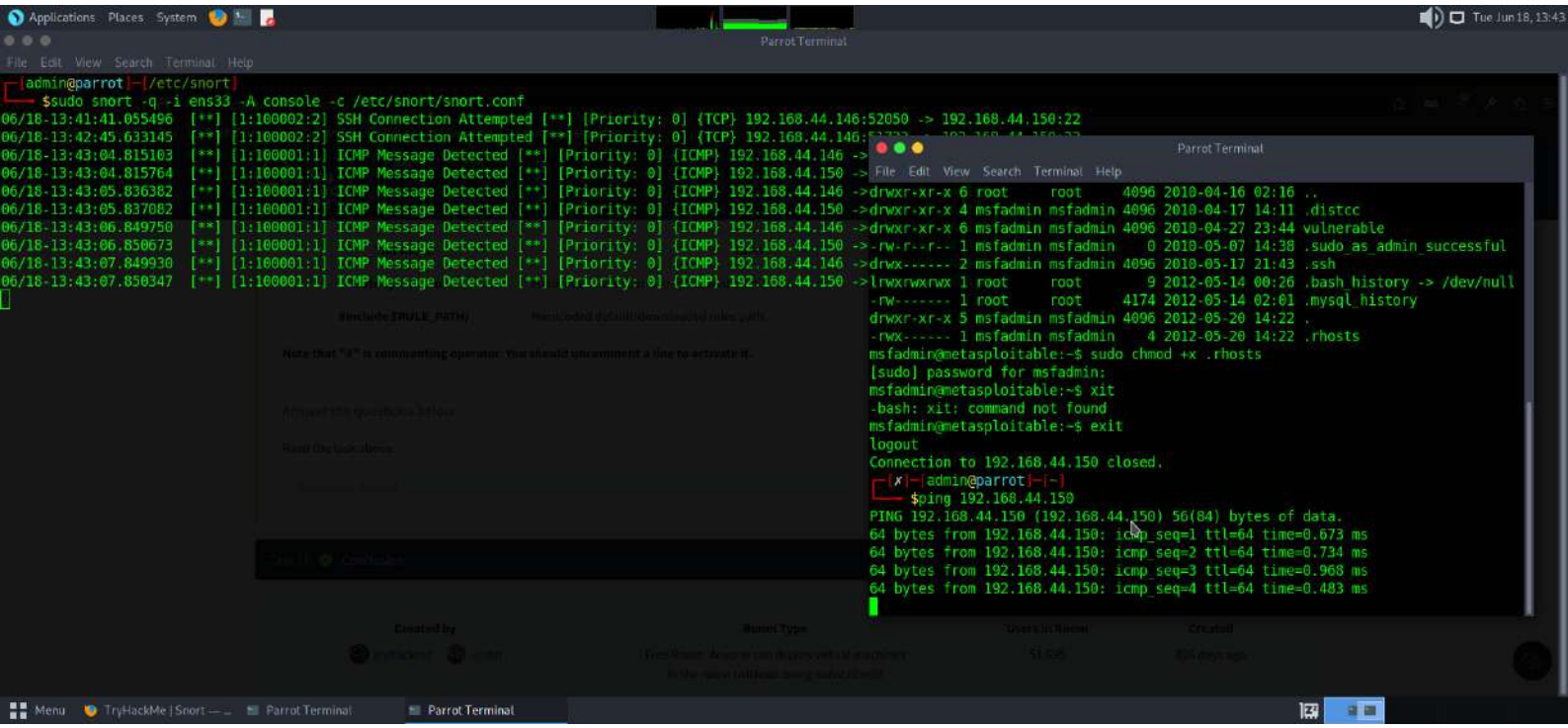
This file intentionally does not come with signatures. Put your local
additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP Message Detected";sid:100001;rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH Connection Attempted";sid:100002;rev:2;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP Connection Detected";sid:100003;priority:2;rev:1;)
[Read 10 lines]
^G Help ^O Read File ^R Replace ^V Paste ^G Go To Line ^Y Redo M-6 Copy ^Q Where Was M-W Next ^ Forward ^ Next Word
^X Exit ^F Where Is ^K Cut ^I Execute ^Z Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^ Prev Word ^A Home
Menu
Parrot Terminal

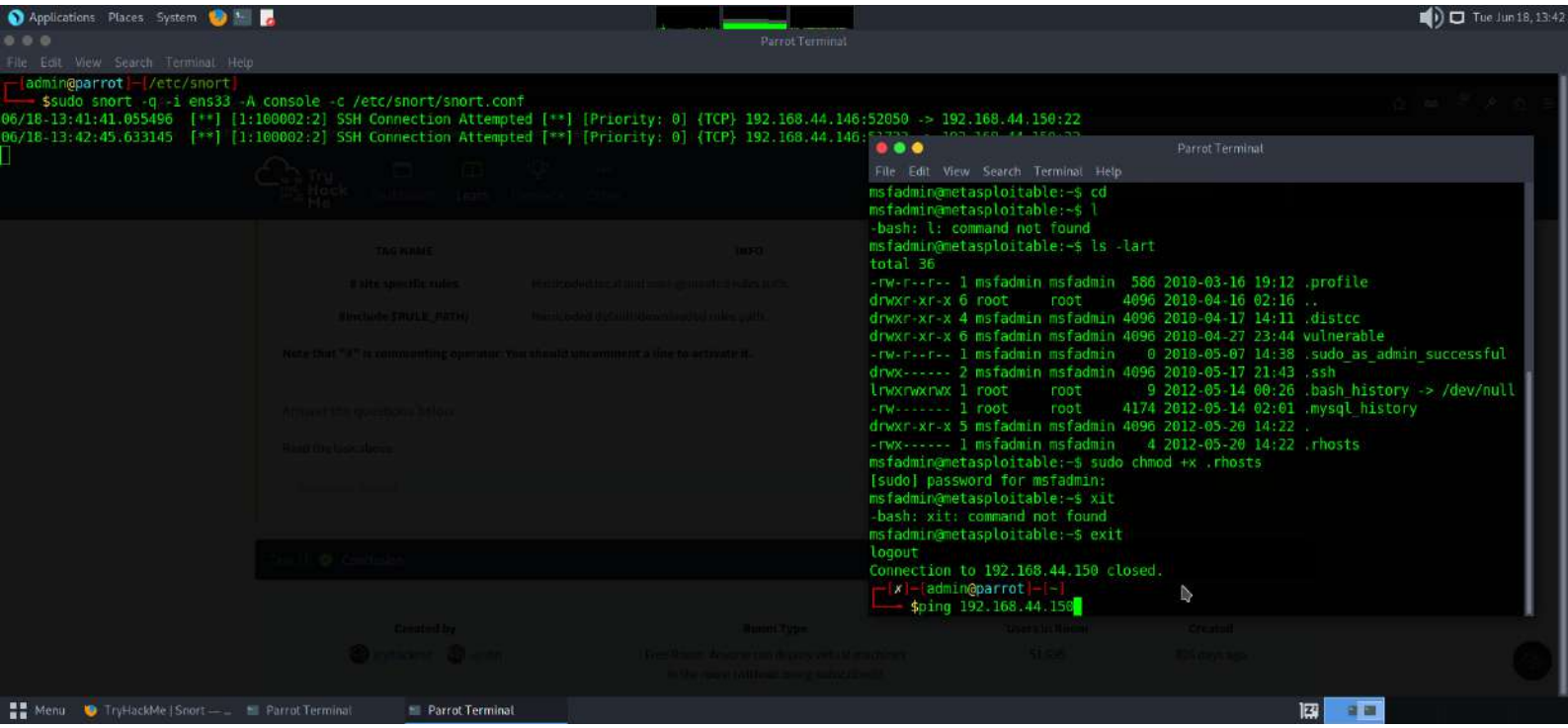

Applications Places System
Mon Jun 17, 14:49
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4 snort.conf
/etc/snort/snort.$interface.conf (where '$interface' is the name of your
network interface) and adjust the valuse there.
#
The Debian init.d script is defined in such a way
that you can run multiple instances.
##
Step #1: Set the network variables. For more information, see README.variables
##
Setup the network addresses you are protecting
#
Note to Debian users: this value is overriden when starting
up the Snort daemon through the init.d script by the
value of DEBIAN_SNORT_HOME_NET s defined in the
/etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.17.0/24
Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
If HOME_NET is defined as something other than "any", alternative, you can
use this definition if you do not want to detect attacks from your internal
IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
List of SMTP servers on your network
[line 77/757 (10%), col 1/39 (2%), char 3028/29785 (10%)]
^G Help ^O Read File ^R Replace ^V Paste ^G Go To Line ^Y Redo M-6 Copy ^Q Where Was M-W Next ^ Forward ^ Next Word
^X Exit ^F Where Is ^K Cut ^T Execute ^Z Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^ Prev Word ^A Home
Menu
Parrot Terminal

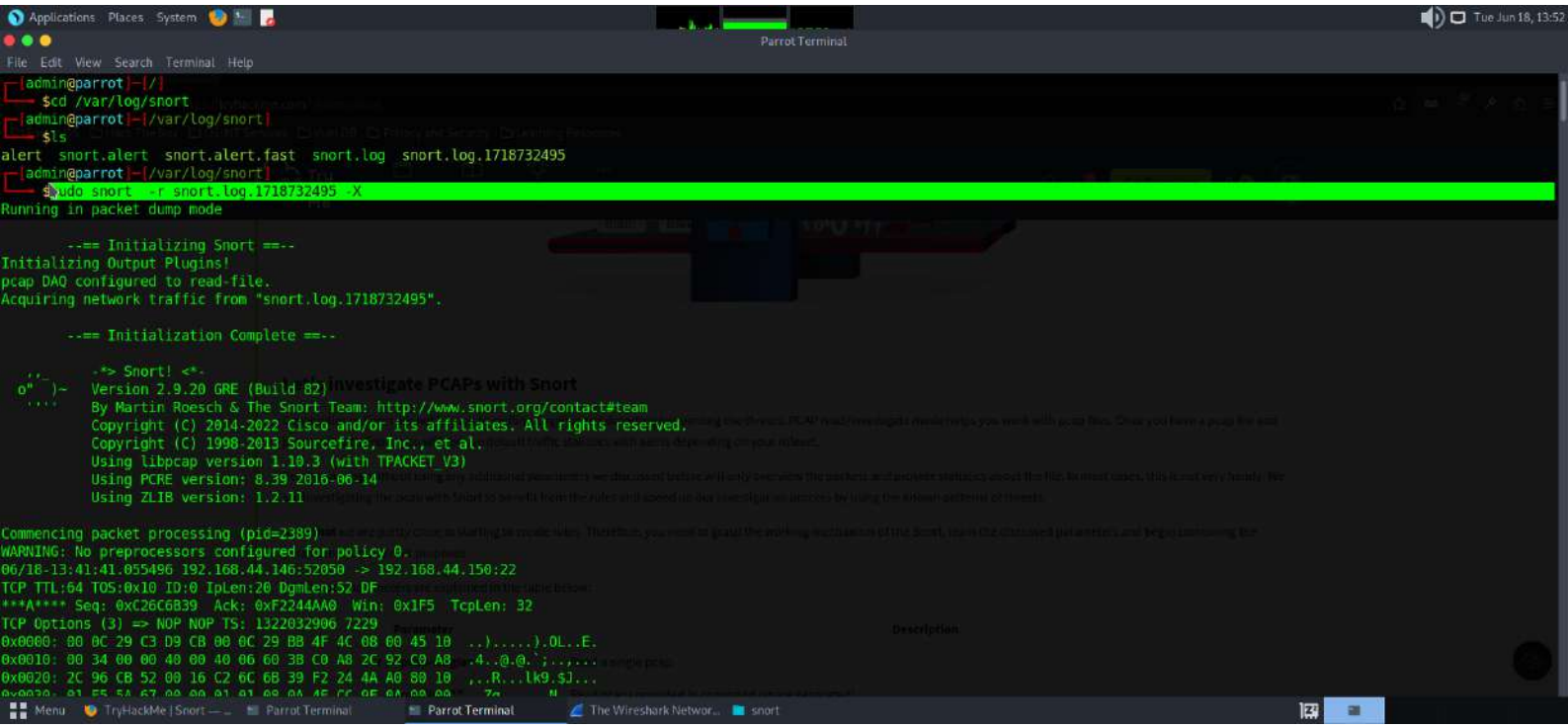

Applications Places System
Tue Jun 18, 13:53
Parrot Terminal
File Edit View Search Terminal Help
GNU nano 5.4
local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

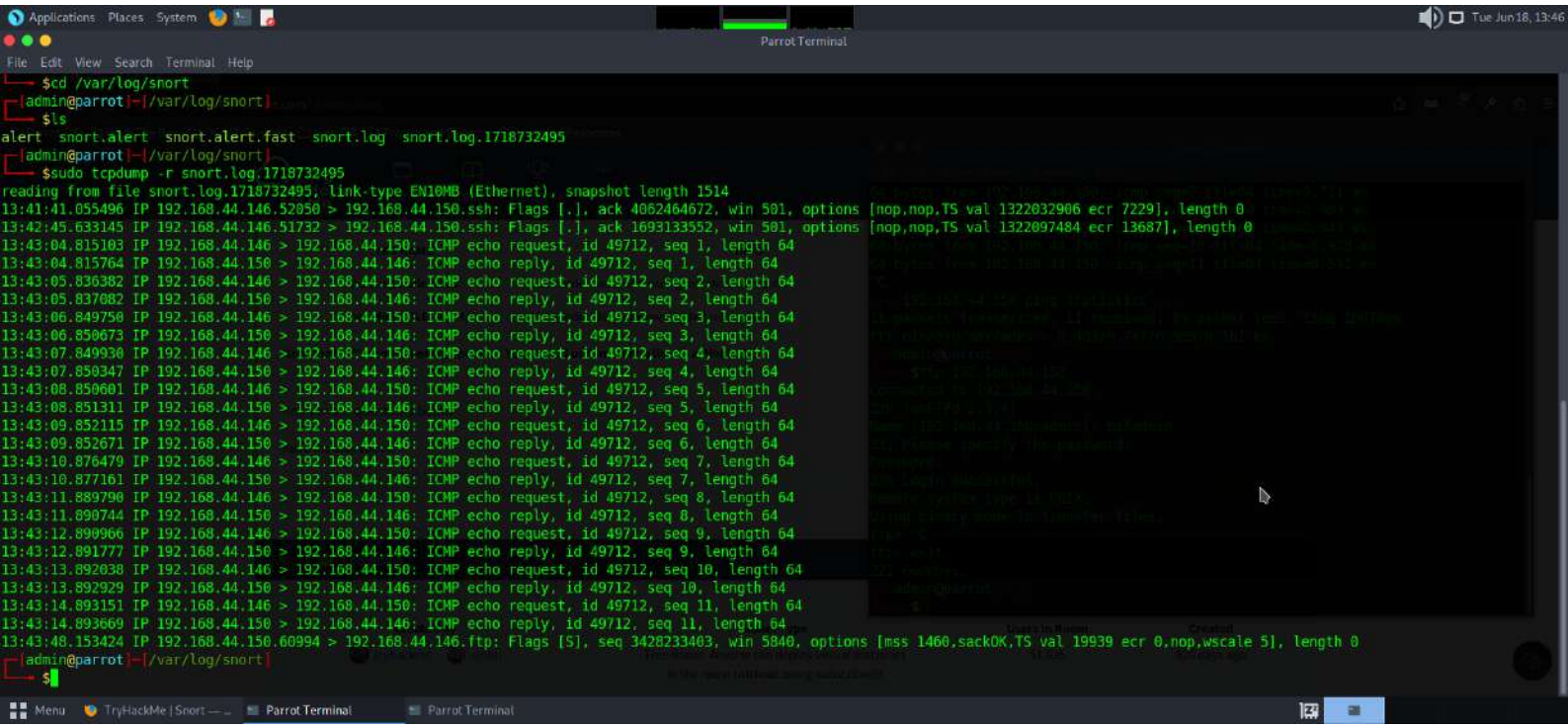
This file intentionally does not come with signatures. Put your local
additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP Message Detected";sid:100001;rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH Connection Attempted";sid:100002;rev:2;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP Connection Detected";sid:100003;priority:2;rev:1;)
Let's investigate PCAPs with Snort
[Read 10 lines]
^G Help
^X Exit
^O Read File
^F Where Is
^R Replace
^K Cut
^V Paste
^J Execute
^C Go To Line
^Z Undo
^Y Redo
M-A Set Mark
M-6 Copy
M-] To Bracket
^Q Where Was
M-Q Previous
M-W Next
^B Back
^ Forward
^ Prev Word
^ Next Word
^A Home
Menu
TryHackMe | Snort — ...
Parrot Terminal
Parrot Terminal
The Wireshark Networ...
snort


Applications Places System
Tue Jun 18, 13:43
Parrot Terminal
File Edit View Search Terminal Help
[admin@parrot]-[/etc/snort]
$sudo snort -q -i ens33 -A console -c /etc/snort/snort.conf
06/18-13:41:41.055496 [**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] {TCP} 192.168.44.146:52050 -> 192.168.44.150:22
06/18-13:42:45.633145 [**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] {TCP} 192.168.44.146:
06/18-13:43:04.815103 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.146 ->
06/18-13:43:04.815764 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.150 ->
06/18-13:43:05.836382 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.146 ->
06/18-13:43:05.837082 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.150 ->
06/18-13:43:06.849750 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.146 ->
06/18-13:43:06.850673 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.150 ->
06/18-13:43:07.849930 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.146 ->
06/18-13:43:07.850347 [**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] {ICMP} 192.168.44.150 ->
Parrot Terminal
File Edit View Search Terminal Help
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw------- 1 root root 4174 2012-05-14 02:01 .mysql_history
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 .
-rwx------ 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
msfadmin@metasploitable:~$ sudo chmod +x .rhosts
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ xit
-bash: xit: command not found
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.44.150 closed.
[admin@parrot]-[~]
$ping 192.168.44.150
PING 192.168.44.150 (192.168.44.150) 56(84) bytes of data.
64 bytes from 192.168.44.150: icmp_seq=1 ttl=64 time=0.673 ms
64 bytes from 192.168.44.150: icmp_seq=2 ttl=64 time=0.734 ms
64 bytes from 192.168.44.150: icmp_seq=3 ttl=64 time=0.968 ms
64 bytes from 192.168.44.150: icmp_seq=4 ttl=64 time=0.483 ms
Menu
TryHackMe | Snort — ...
Parrot Terminal
Parrot Terminal


Applications Places System
Tue Jun 18, 13:42
Parrot Terminal
File Edit View Search Terminal Help
[admin@parrot]-[/etc/snort]
$sudo snort -q -i ens33 -A console -c /etc/snort/snort.conf
06/18-13:41:41.055496 [**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] {TCP} 192.168.44.146:52050 -> 192.168.44.150:22
06/18-13:42:45.633145 [**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] {TCP} 192.168.44.146:
Parrot Terminal
File Edit View Search Terminal Help
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ l
-bash: l: command not found
msfadmin@metasploitable:~$ ls -lart
total 36
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw------- 1 root root 4174 2012-05-14 02:01 .mysql_history
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 .
-rwx------ 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
msfadmin@metasploitable:~$ sudo chmod +x .rhosts
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ xit
-bash: xit: command not found
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.44.150 closed.
[x]-[admin@parrot]-[~]
$ping 192.168.44.150
Menu
TryHackMe | Snort — ...
Parrot Terminal
Parrot Terminal


Applications Places System
Tue Jun 18, 13:52
Parrot Terminal
File Edit View Search Terminal Help
[admin@parrot]-[/]
$cd /var/log/snort
[admin@parrot]-[/var/log/snort]
$ls
alert snort.alert snort.alert.fast snort.log snort.log.1718732495
[admin@parrot]-[/var/log/snort]
$sudo snort -r snort.log.1718732495 -X
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
Acquiring network traffic from "snort.log.1718732495".
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.3 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2389)
WARNING: No preprocessors configured for policy 0.
06/18-13:41:41.055496 192.168.44.146:52050 -> 192.168.44.150:22
TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
A* Seq: 0xC26C6B39 Ack: 0xF2244AA0 Win: 0x1F5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1322032906 7229
0x0000: 00 0C 29 C3 D9 CB 00 0C 29 BB 4F 4C 08 00 45 10 ..)....).OL..E.
0x0010: 00 34 00 00 40 00 40 06 60 3B C0 A8 2C 92 C0 A8 .4..@.@.`;..,...
0x0020: 2C 96 CB 52 00 16 C2 6C 6B 39 F2 24 4A A0 80 10 ,..R...lk9.$J...
Menu
TryHackMe | Snort — ...
Parrot Terminal
Parrot Terminal
The Wireshark Networ...
snort


Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
Commencing packet processing (pid=2389)
WARNING: No preprocessors configured for policy 0.
06/18-13:41:41.055496 192.168.44.146:52050 -> 192.168.44.150:22
TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
A* Seq: 0xC26C6B39 Ack: 0xF2244AA0 Win: 0x1F5 TcpLen: 32
0x0000: 00 0C 29 C3 D9 CB 00 0C 29 BB 4F 4C 08 00 45 10 ..)......).OL..E.
0x0010: 00 34 00 00 40 00 40 06 60 3B C0 A8 2C 92 C0 A8 .4..@.@.`;..,...
0x0020: 2C 96 CB 52 00 16 C2 6C 6B 39 F2 24 4A A0 80 10 ,..R...lk9.$J...
0x0030: 01 F5 5A 67 00 00 01 01 08 0A 4E CC 9F 0A 00 00 ..Zg......N.....
0x0040: 1C 3D .=
=+
WARNING: No preprocessors configured for policy 0.
06/18-13:42:45.633145 192.168.44.146:51732 -> 192.168.44.150:22
TCP TTL:64 TOS:0x10 ID:0 IpLen:20 DgmLen:52 DF
A* Seq: 0x7614F783 Ack: 0x64EB2AF0 Win: 0x1F5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1322097484 13687
0x0000: 00 0C 29 C3 D9 CB 00 0C 29 BB 4F 4C 08 00 45 10 ..)......).OL..E.
0x0010: 00 34 00 00 40 00 40 06 60 3B C0 A8 2C 92 C0 A8 .4..@.@.`;..,...
0x0020: 2C 96 CA 14 00 16 76 14 F7 83 64 EB 2A F0 80 10 ,.....v...d.*...
0x0030: 01 F5 B3 1F 00 00 01 01 08 0A 4E CD 9B 4C 00 00 ..........N..L..
0x0040: 35 77 5w
=+
WARNING: No preprocessors configured for policy 0.
06/18-13:43:04.815103 192.168.44.146 -> 192.168.44.150
ICMP TTL:64 TOS:0x0 ID:56803 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:49712 Seq:1 ECHO
0x0000: 00 0C 29 C3 D9 CB 00 0C 29 BB 4F 4C 08 00 45 00 ..)......).OL..E.
0x0010: 00 54 DD E3 40 00 40 01 82 4C C0 A8 2C 92 C0 A8 .T..@.@..L..,...
Menu TryHackMe | Snort — ... Parrot Terminal Parrot Terminal The Wireshark Networ... snort


Applications Places System
Tue Jun 18, 13:46
Parrot Terminal
File Edit View Search Terminal Help
$cd /var/log/snort
[admin@parrot]-[/var/log/snort]
$ls
alert snort.alert snort.alert.fast snort.log snort.log.1718732495
[admin@parrot]-[/var/log/snort]
$sudo tcpdump -r snort.log.1718732495
reading from file snort.log.1718732495, link-type EN10MB (Ethernet), snapshot length 1514
13:41:41.055496 IP 192.168.44.146.52050 > 192.168.44.150.ssh: Flags [.], ack 4062464672, win 501, options [nop,nop,TS val 1322032906 ecr 7229], length 0
13:42:45.633145 IP 192.168.44.146.51732 > 192.168.44.150.ssh: Flags [.], ack 1693133552, win 501, options [nop,nop,TS val 1322097484 ecr 13687], length 0
13:43:04.815103 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 1, length 64
13:43:04.815764 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 1, length 64
13:43:05.836382 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 2, length 64
13:43:05.837082 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 2, length 64
13:43:06.849750 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 3, length 64
13:43:06.850673 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 3, length 64
13:43:07.849930 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 4, length 64
13:43:07.850347 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 4, length 64
13:43:08.850601 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 5, length 64
13:43:08.851311 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 5, length 64
13:43:09.852115 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 6, length 64
13:43:09.852671 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 6, length 64
13:43:10.876479 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 7, length 64
13:43:10.877161 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 7, length 64
13:43:11.889790 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 8, length 64
13:43:11.890744 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 8, length 64
13:43:12.890966 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 9, length 64
13:43:12.891777 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 9, length 64
13:43:13.892038 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 10, length 64
13:43:13.892929 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 10, length 64
13:43:14.893151 IP 192.168.44.146 > 192.168.44.150: ICMP echo request, id 49712, seq 11, length 64
13:43:14.893669 IP 192.168.44.150 > 192.168.44.146: ICMP echo reply, id 49712, seq 11, length 64
13:43:48.153424 IP 192.168.44.150.60994 > 192.168.44.146.ftp: Flags [S], seq 3428233403, win 5840, options [mss 1460,sackOK,TS val 19939 ecr 0,nop,wscale 5], length 0
[admin@parrot]-[/var/log/snort]
$
Menu
TryHackMe | Snort — ...
Parrot Terminal
Parrot Terminal

Search Tab in Splunk:-

1- Selected Fields : Splunk extracts the default fields like source, sourcetype, and host, which appear in each event, and places them under the selected fields column. We can select other fields that seem essential and add them to the list.
2- Interesting Fields Pulls all the interesting fields it finds and displays them in the left panel to further explore.
3- Alpha-numeric fields 'α' This alpha symbol shows that the field contains text values.
4- Numeric fields '#' This symbol shows that this field contains numerical values.
5- Count The number against each field shows the number of events captured in that timeframe.

Splunk Search Processing Language comprises of multiple functions, operators and commands that are used together to form a simple to complex search and get the desired results from the ingested logs.
Splunk field operators are the building blocks used to construct any search query. These field operators are used to filter, remove, and narrow down the search result based on the given criteria. Common field operators are Comparison operators, wildcards, and boolean operators.
Comparison Operators:-
These operators are used to compare the values against the fields. Some common comparisons operators are mentioned below:
Field Name
UserName=Mark This operator is used to match values against the field. In this example, it will look for all the events, where the value of the field UserName is equal to Mark.
Not Equal to
!=
UserName!=Mark This operator returns all the events where the UserName value does not match Mark.
Less than:Age < 10 Showing all the events with the value of Age less than 10.
Less than or Equal to<= :Age <= 10 Showing all the events with the value of Age less than or equal to 10.
Greater than> :Outbound_traffic > 50 MB This will return all the events where the Outbound traffic value is over 50 MB.
Greater Than or Equal to>=:Outbound_traffic >= 50 MB
Example:-Search Query: index=windowslogs AccountName !=SYSTEM

Boolean Operators

Splunk supports the following Boolean operators, which can be very handy in searching/filtering and narrowing down result.

NOT

field_A NOT value

Ignore the events from the result where field_A contain the specified value.

OR

field_A=value1 OR field_A=value2

Return all the events in which field_A contains either value1 or value2.

AND

field_A=value1 AND field_B=value2Return all the events in which field_A contains value1 and field_B contains value2.

To understand how boolean operator works in SPL, lets add the condition to show the events from the James account.

Search Query: index=windowslogs AccountName !=SYSTEM AND AccountName=James

Our network generates thousands of logs each minute, all ingesting into our SIEM solution. It becomes a daunting task to search for any anomaly without using filters. SPL allows us to use Filters to narrow down the result and only show the important events that we are interested in. We can add or remove certain data from the result using filters. The following commands are useful in applying filters to the search results.

Command

1.fields

Explanation:Fields command is used to add or remove mentioned fields from the search results. To remove the field, minus sign (-) is used before the fieldname and plus (+) is used before the fields which we want to display.Syntax | fields <field_name1> <field_name2> Example : | fields + HostName - EventID

Command

2.search

Explanation :This command is used to search for the raw text while using the chaining command | ; Syntax :| search <search_keyword> ; Example :| search "Powershell"
Search Query: index=windowslogs | search Powershell

3.dedup

Explanation

Dedup is the command used to remove duplicate fields from the search results. We often get the results with various fields getting the same results. These commands remove the duplicates to show the unique values. Syntax | dedup <fieldname> ;Example:| dedup EventID.

4.rename

Explanation

It allows us to change the name of the field in the search results. It is useful in a scenario when the field name is generic or log, or it needs to be updated in the output.
Syntax :| rename <fieldname> ;Example :| rename User as Employees

5.Each event has multiple fields, and not every field is important to display. The Table command allows us to create a table with selective fields as columns.

Syntax

| table <field_name1> <fieldname_2> ; Example | table | head 20 # will return the top 20 events from the result list.

6.Head

Explanation

The head command returns the first 10 events if no number is specified.

Syntax

| head <number> ; Example| head # will return the top 10 events from the result list ;| head 20 # will return the top 20 events from the result list

Criteria	Splunk	Spark
Deployment area	Collecting large amounts of machine-generated data	Iterative applications and in-memory processing
Nature of tool	Proprietary	Open-source
Working mode	Streaming mode	Both streaming and batch modes

2. What is Splunk?
Splunk is 'Google' for our machine-generated data. It's a software/engine that can be used for searching, visualizing, monitoring, reporting, etc. of our enterprise data. Splunk takes valuable machine data and turns it into powerful operational intelligence by providing real-time insights into our data through charts, alerts, reports, etc.

Service	Port Number Used
Splunk Web port	8000
Splunk Management port	8089
Splunk Indexing port	9997
Splunk Index Replication port	8080
Splunk Network port	514 (Used to get data from the Network port, i.e., UDP data)
KV Store	8191

4. What are the components of Splunk? Explain Splunk architecture.
This is one of the most frequently asked Splunk interview questions. Below are the components of Splunk:
Search Head: Provides the GUI for searching
Indexer: Indexes the machine data
Forwarder: Forwards logs to the Indexer.
Deployment Server: Manages Splunk components in a distributed environment.
5. Which is the latest Splunk version in use? : Splunk 8.2.1 (as of June 21, 2021)
6.name a few most important configuration files in Splunk?
props.conf indexes.conf inputs.conf transforms.conf server.conf
7. What are the types of Splunk Licenses?
Enterprise license
Free license
Forwarder license
Beta license
Licenses for search heads (for distributed search)
Licenses for cluster members (for index replication

How to reset the Splunk admin password?
Resetting the Splunk admin password depends on the version of Splunk. If we are using Splunk 7.1 and above, then we have to follow the below steps:

First, we have to stop our Splunk Enterprise
Now, we need to find the 'passwd' file and rename it to 'passwd.bk'
Then, we have to create a file named 'user-seed.conf' in the below directory:
1
$SPLUNK_HOME/etc/system/local/
In the file, we will have to use the following command (here, in place of 'NEW_PASSWORD', we will add our own new password):

[user_info]

PASSWORD = NEW_PASSWORD
After that, we can just restart the Splunk Enterprise and use the new password to log in How are forwarder licenses purchased?
They are included in Splunk. Therefore, there is no need to purchase them separately.

Interested in learning Splunk? Go for the online instructor-led Splunk Training in Toronto!

25. What is the command for restarting Splunk web server?
This is another frequently asked Splunk commands interview question. Get a thorough idea of commands We can restart the Splunk web server by using the following command:

splunk start splunkweb
26. What is the command for restarting the Splunk Daemon?
Splunk Deamon can be restarted with the below command:

1
splunk start splunkd
27. What is the command used to check the running Splunk processes on Unix/Linux?
If we want to check the running Splunk Enterprise processes on Unix/Linux, we can make use of the following command:

1
ps aux | grep splunk

What is SIEM

SIEM stands for Security Information and Event Management system. It is a tool that collects data from various endpoints/network devices across the network, stores them at a centralized place, and performs correlation on them. This room will cover the basic concepts required to understand SIEM and how it works.
Two major types of Log Source:-
1) Host-Centric Log Sources

These are log sources that capture events that occurred within or related to the host. Some log sources that generate host-centric logs are Windows Event logs, Sysmon, Osquery, etc. Some examples of host-centric logs are:

A user accessing a file
A user attempting to authenticate.
A process Execution Activity
A process adding/editing/deleting a registry key or value.
Powershell execution
2) Network-Centric Log Sources

Network-related logs are generated when the hosts communicate with each other or access the internet to visit a website. Some network-based protocols are SSH, VPN, HTTP/s, FTP, etc. Examples of such events are:

SSH connection
A file being accessed via FTP
Web traffic
A user accessing company's resources through VPN.
Network file sharing Activity

Importance of SIEM:-
Now that we have covered various types of logs, it's time to understand the importance of SIEM. As all these devices generate hundreds of events per second, examining the imglogs on each device one by one in case of any incident can be a tedious task. That is one of the advantages of having a SIEM solution in place. It not only takes logs from various sources in real-time but also provides the ability to correlate between events, search through the logs, investigate incidents and respond promptly. Some key features provided by SIEM are:
Real-time log ingestion
Alerting against abnormal activities
24/7 Monitoring and visibility
Protection against the latest threats through early detection
Data Insights and visualization
Ability to investigate past incidents.

Linux Workstation

Linux OS stores all the related logs, such as events, errors, warnings, etc. Which are then ingested into SIEM for continuous monitoring. Some of the common locations where Linux store logs are:

/var/log/httpd : Contains HTTP Request / Response and error logs.
/var/log/cron : Events related to cron jobs are stored in this location.
/var/log/auth.log and /var/log/secure : Stores authentication related logs.
/var/log/kern : This file stores kernel related events.

Log Injestion:-
All these logs provide a wealth of information and can help in identifying security issues. Each SIEM solution has its own way of ingesting the logs. Some common methods used by these SIEM solutions are explained below:

1] Agent / Forwarder: These SIEM solutions provide a lightweight tool called an agent (forwarder by Splunk) that gets installed in the Endpoint. It is configured to capture all the important logs and send them to the SIEM server.

2] Syslog: Syslog is a widely used protocol to collect data from various systems like web servers, databases, etc., are sent real-time data to the centralized destination.
3] Manual Upload: Some SIEM solutions, like Splunk, ELK, etc., allow users to ingest offline data for quick analysis. Once the data is ingested, it is normalized and made available for analysis.

4] Port-Forwarding: SIEM solutions can also be configured to listen on a certain port, and then the endpoints forward the data to the SIEM instance on the listening port.

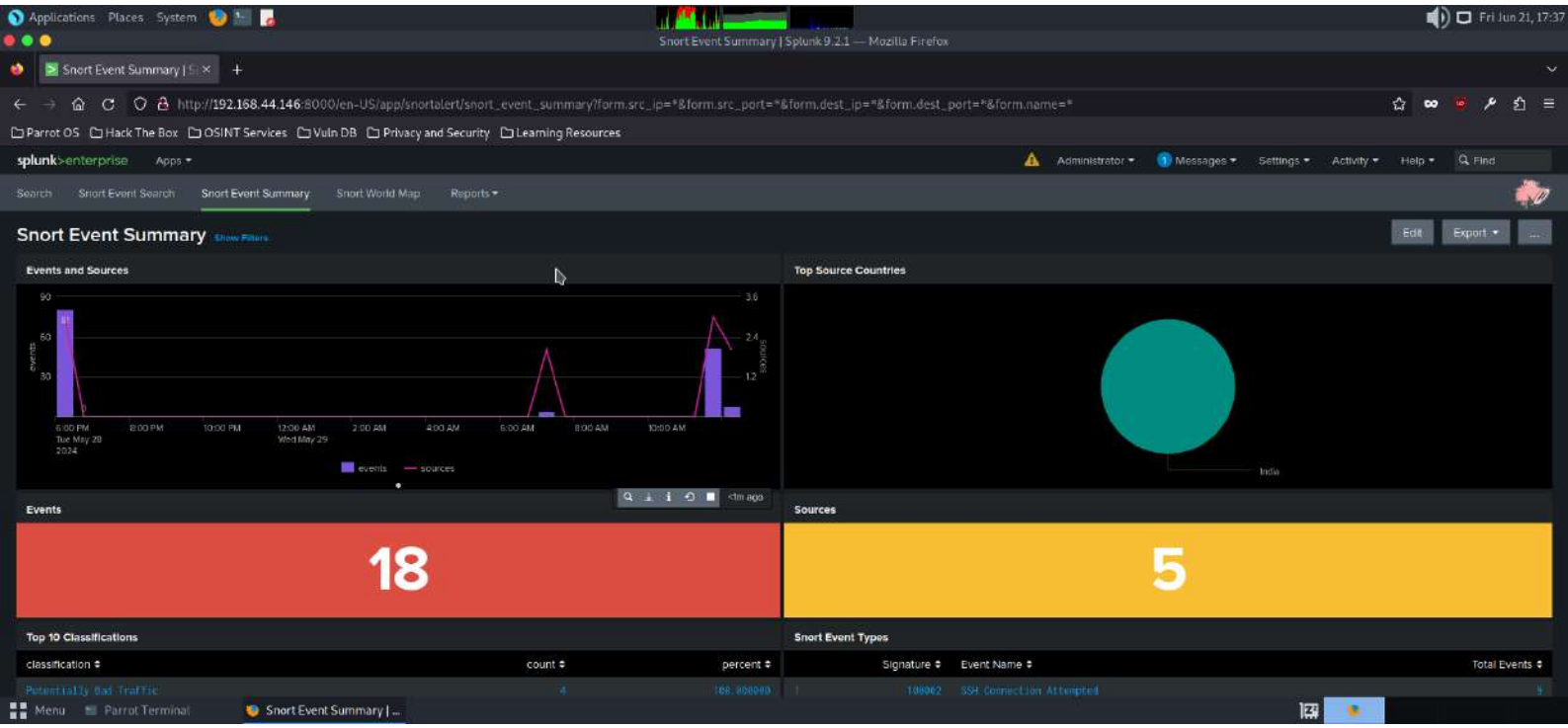
SOC Analyst Responsibilities

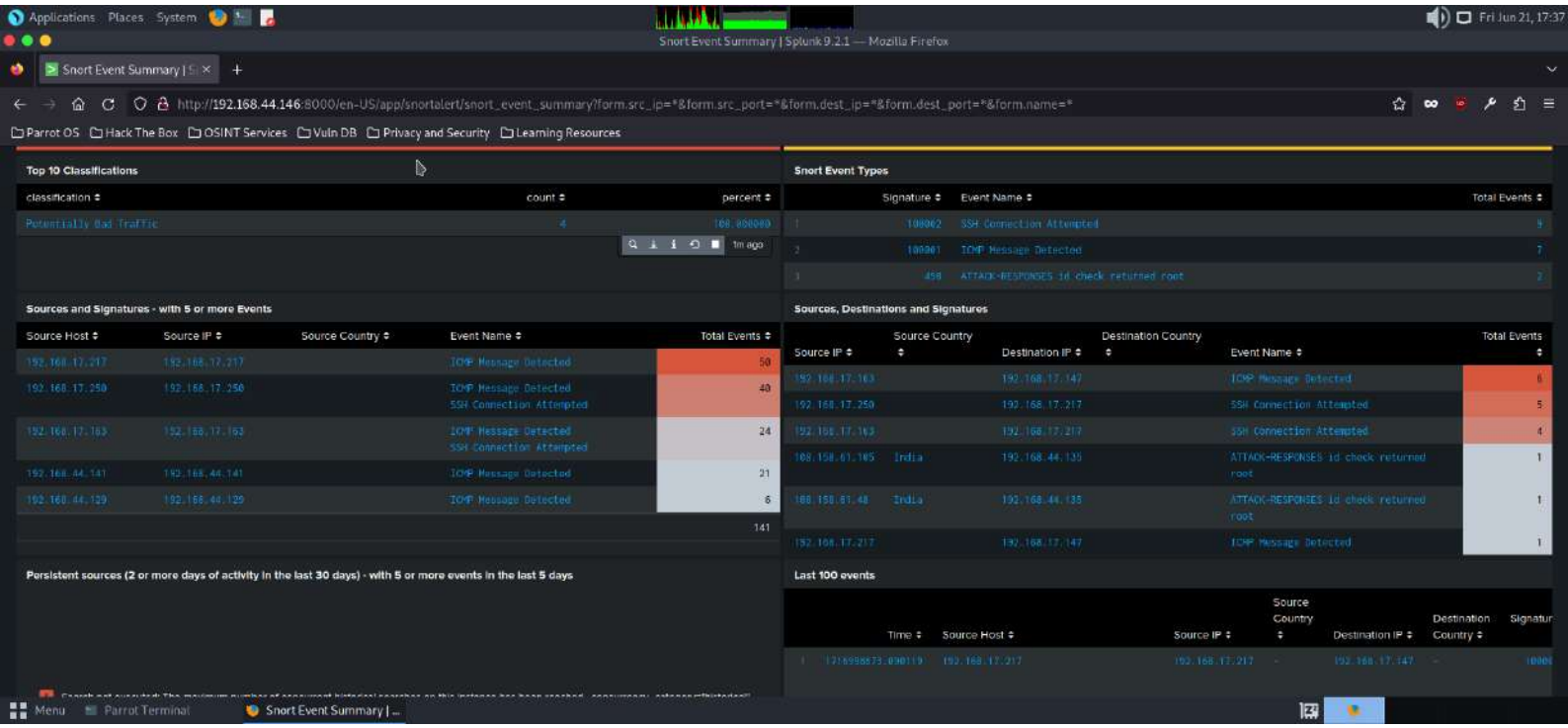
SOC Analysts utilize SIEM solutions in order to have better visibility of what is happening within the network. Some of their responsibilities include:

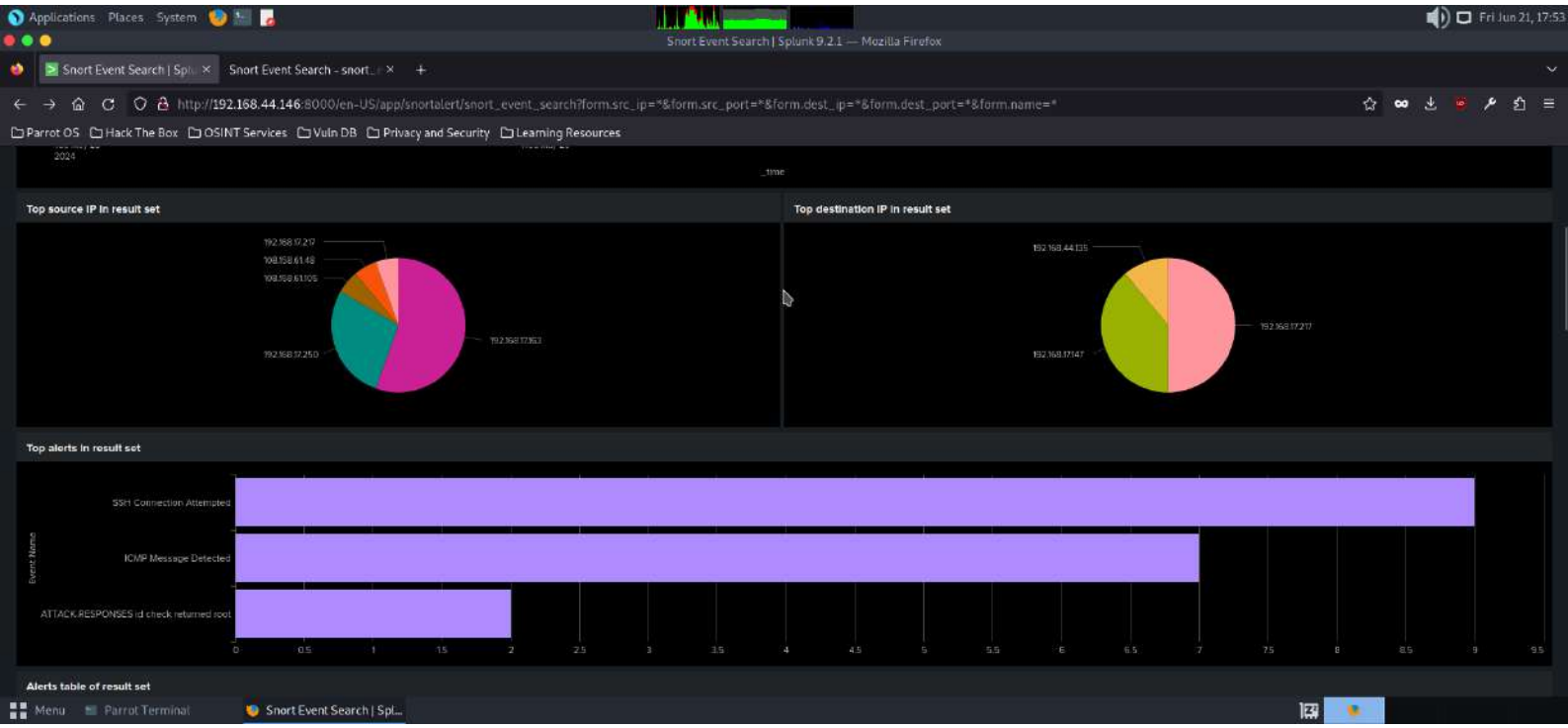
Monitoring and Investigating.
Identifying False positives.
Tuning Rules which are causing the noise or False positives.
Reporting and Compliance.
Identifying blind spots in the network visibility and covering them.

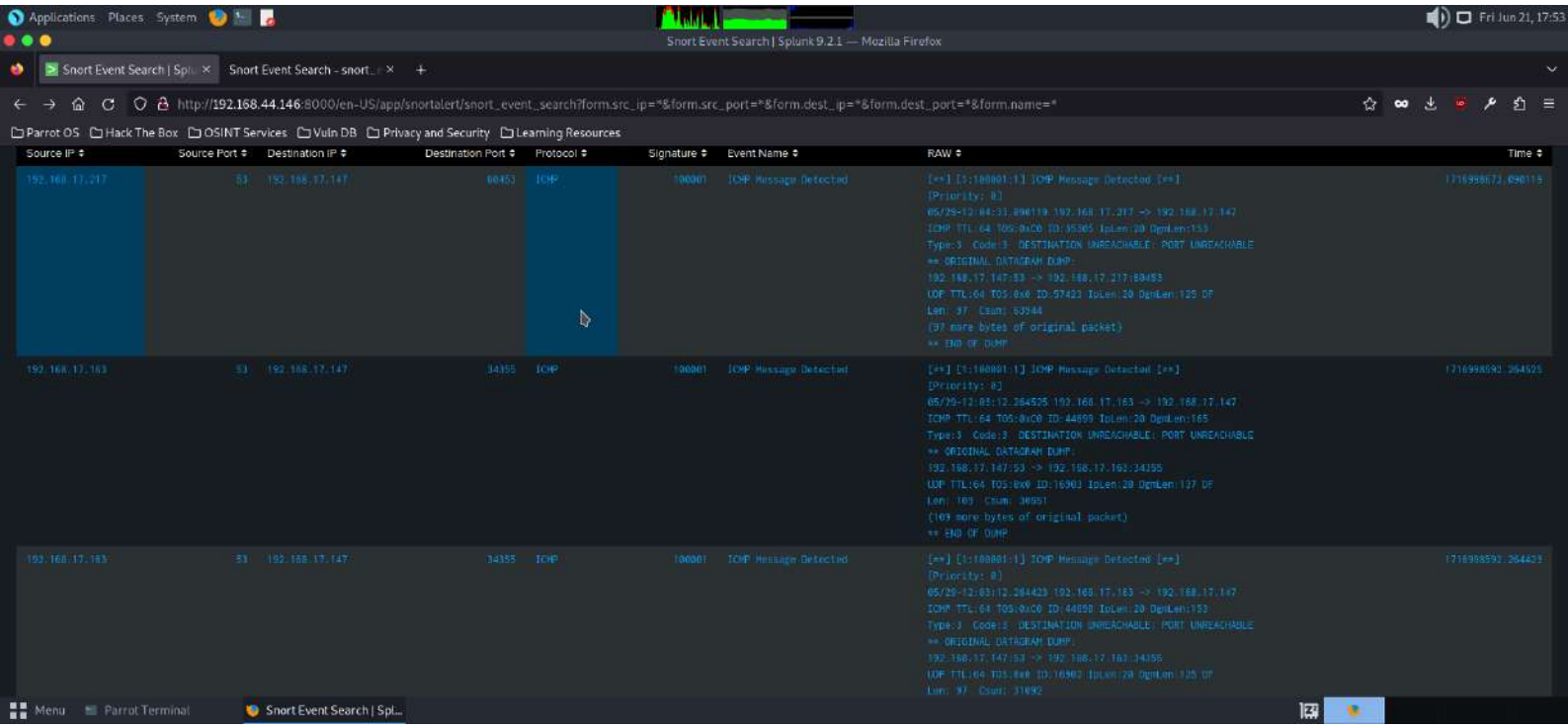

Applications Places System
Fri Jun 21, 17:34
Parrot Terminal
File Edit View Search Terminal Help
[admin@parrot]-[~]
$cd .
[admin@parrot]-[~]
$cd ..
[admin@parrot]-[/home]
$cd ..
[admin@parrot]-[/]
$cd /opt/splunk/bin
[admin@parrot]-[/opt/splunk/bin]
$sudo ./splunk start
[sudo] password for admin:
splunkd 1730 was not running.
Stopping splunk helpers...
Done.
Stopped helpers.
Removing stale pid file... done.
Splunk> Winning the War on Error
Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
Checking appserver port [127.0.0.1:8065]: open
Checking kvstore port [8191]: open
Checking configuration... Done.
Checking critical directories... Done
Checking indexes...
Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Menu
Parrot Terminal
Mozilla Firefox

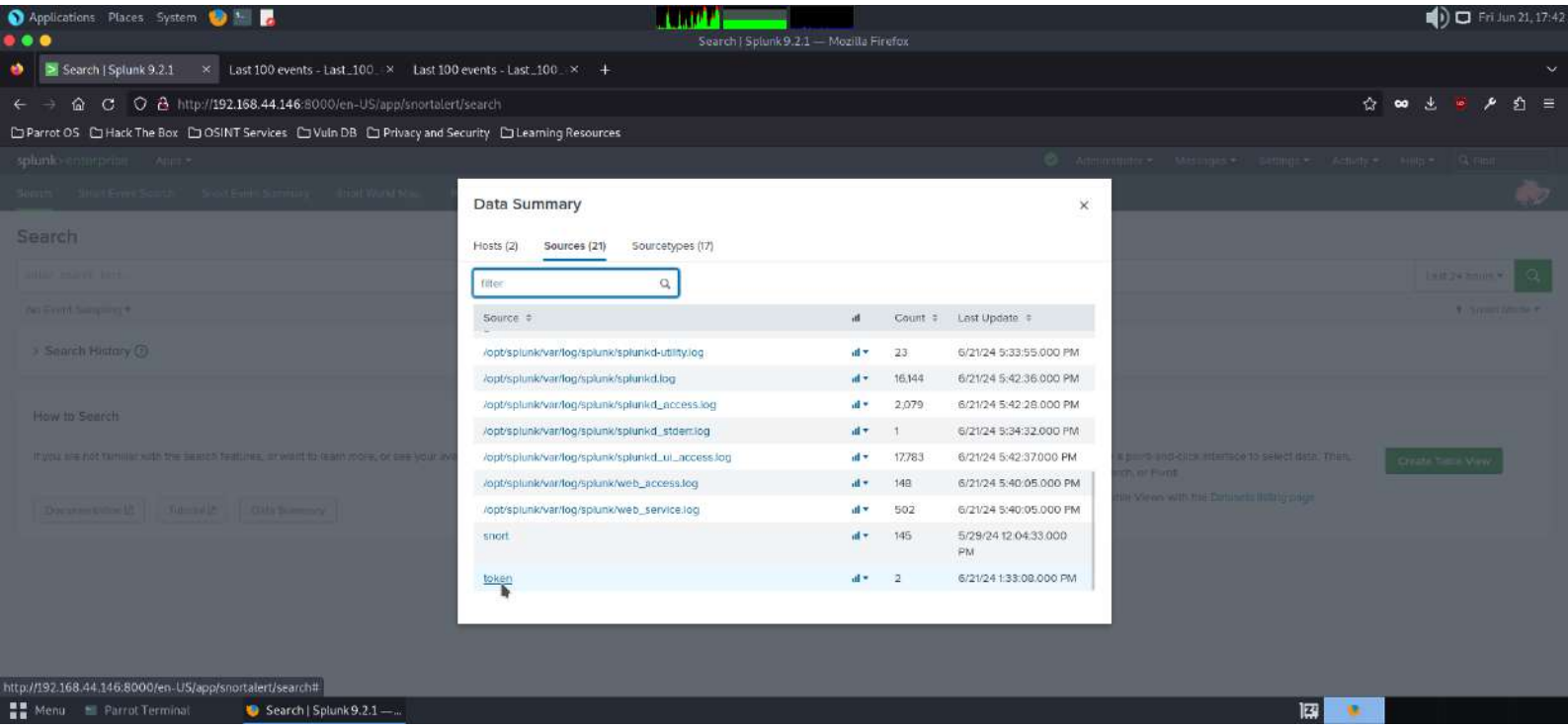

Applications Places System
Fri Jun 21, 17:34
Parrot Terminal
File Edit View Search Terminal Help
Checking http port [8000]: open
Checking mgmt port [8089]: open
Checking appserver port [127.0.0.1:8065]: open
Checking kvstore port [8191]: open
Checking configuration... Done.
Checking critical directories... Done
Checking indexes...
Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://parrot:8000
[admin@parrot]-[/opt/splunk/bin]
$
Menu
Parrot Terminal
Mozilla Firefox

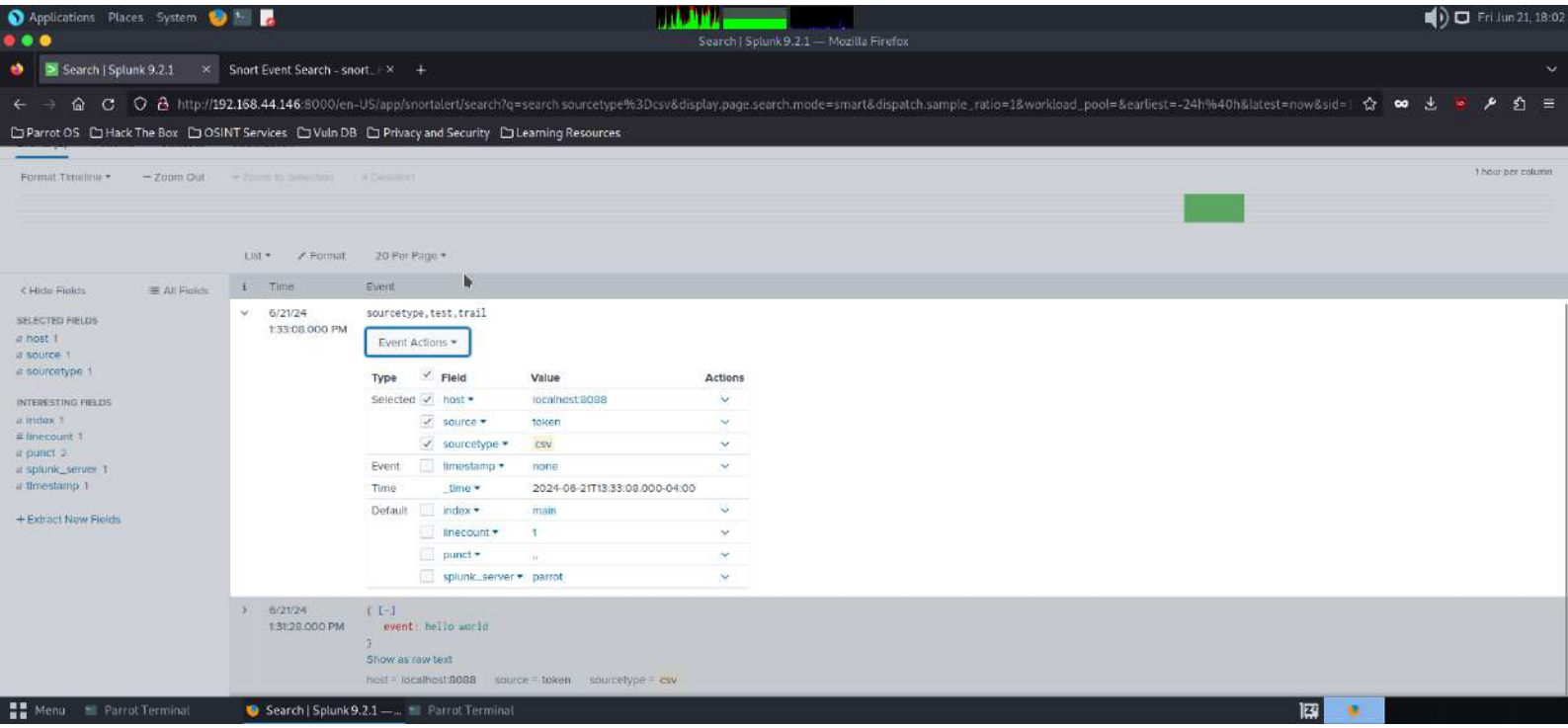

Applications Places System
Fri Jun 21, 17:37
Snort Event Summary | Splunk 9.2.1 — Mozilla Firefox
Snort Event Summary | S
http://192.168.44.146:8000/en-US/app/snortalert/snort_event_summary?form.src_ip=*&form.src_port=*&form.dest_ip=*&form.dest_port=*&form.name=*
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Snort Event Search
Snort Event Summary
Snort World Map
Reports
Snort Event Summary
Show Filters
Edit
Export
Events and Sources
events
sources
6:00 PM Tue May 28 2024
8:00 PM
10:00 PM
12:00 AM Wed May 29
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
Top Source Countries
India
Events
18
Sources
5
Top 10 Classifications
classification
count
percent
Potentially Bad Traffic
4
100.000000
Snort Event Types
Signature
Event Name
Total Events
1
100002
SSH Connection Attempted
5
Menu
Parrot Terminal
Snort Event Summary | ...

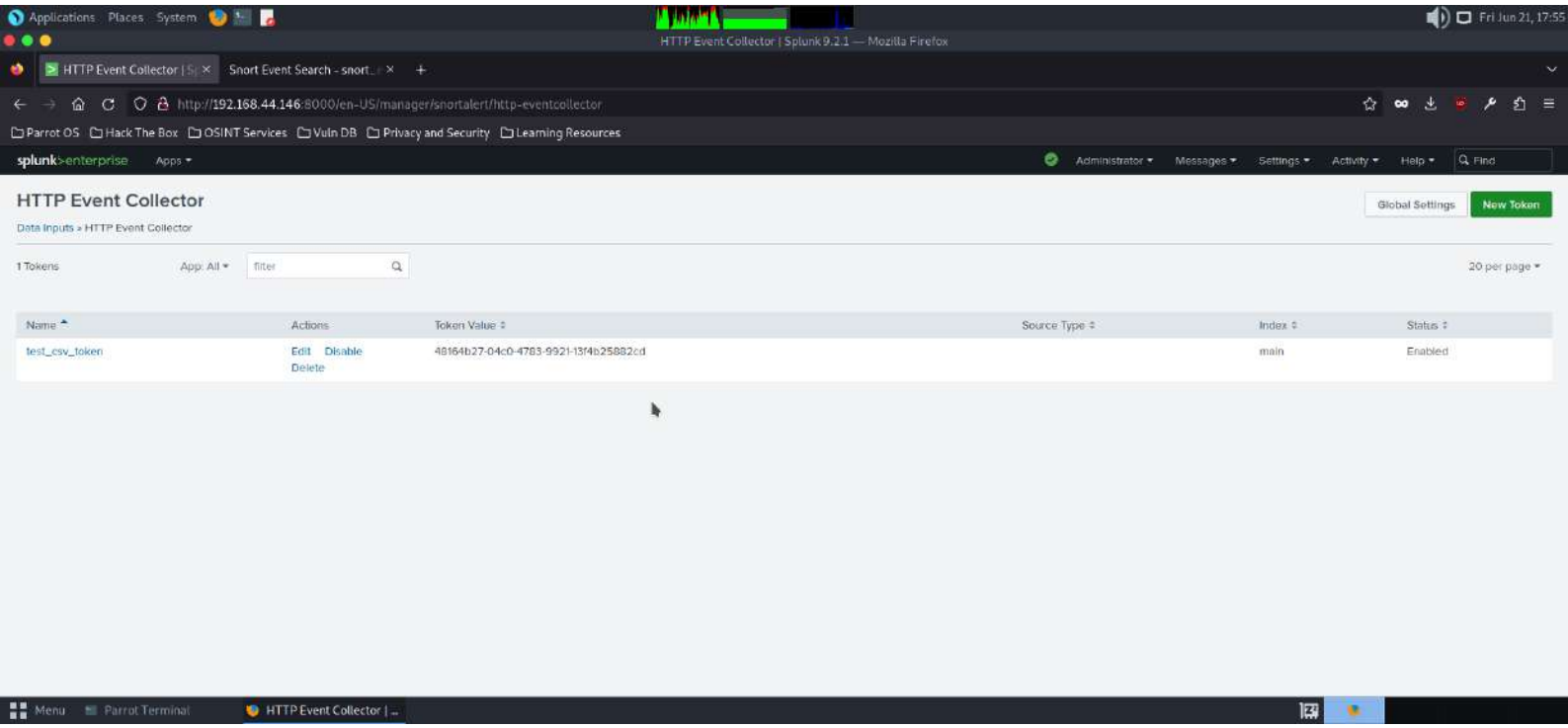

Applications Places System
Fri Jun 21, 17:37
Snort Event Summary | Splunk 9.2.1 — Mozilla Firefox
Snort Event Summary | S
http://192.168.44.146:8000/en-US/app/snortalert/snort_event_summary?form.src_ip=*&form.src_port=*&form.dest_ip=*&form.dest_port=*&form.name=*
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Top 10 Classifications
classification
count
percent
Potentially Bad Traffic
4
100.000000
1m ago
Snort Event Types
Signature
Event Name
Total Events
1
100002
SSH Connection Attempted
9
2
100001
ICMP Message Detected
7
3
498
ATTACK-RESPONSES id check returned root
2
Sources and Signatures - with 5 or more Events
Source Host
Source IP
Source Country
Event Name
Total Events
192.168.17.217
192.168.17.217
ICMP Message Detected
50
192.168.17.250
192.168.17.250
ICMP Message Detected
SSH Connection Attempted
40
192.168.17.163
192.168.17.163
ICMP Message Detected
SSH Connection Attempted
24
192.168.44.141
192.168.44.141
ICMP Message Detected
21
192.168.44.129
192.168.44.129
ICMP Message Detected
6
141
Sources, Destinations and Signatures
Source IP
Source Country
Destination IP
Destination Country
Event Name
Total Events
192.168.17.163
192.168.17.147
ICMP Message Detected
6
192.168.17.250
192.168.17.217
SSH Connection Attempted
5
192.168.17.163
192.168.17.217
SSH Connection Attempted
4
188.158.61.105
India
192.168.44.135
ATTACK-RESPONSES id check returned root
1
188.158.81.48
India
192.168.44.135
ATTACK-RESPONSES id check returned root
1
192.168.17.217
192.168.17.147
ICMP Message Detected
1
Persistent sources (2 or more days of activity in the last 30 days) - with 5 or more events in the last 5 days
Last 100 events
Time
Source Host
Source IP
Source Country
Destination IP
Destination Country
Signatur
1
1718998873.090119
192.168.17.217
192.168.17.217
-
192.168.17.147
-
10000
Menu
Parrot Terminal
Snort Event Summary | ...

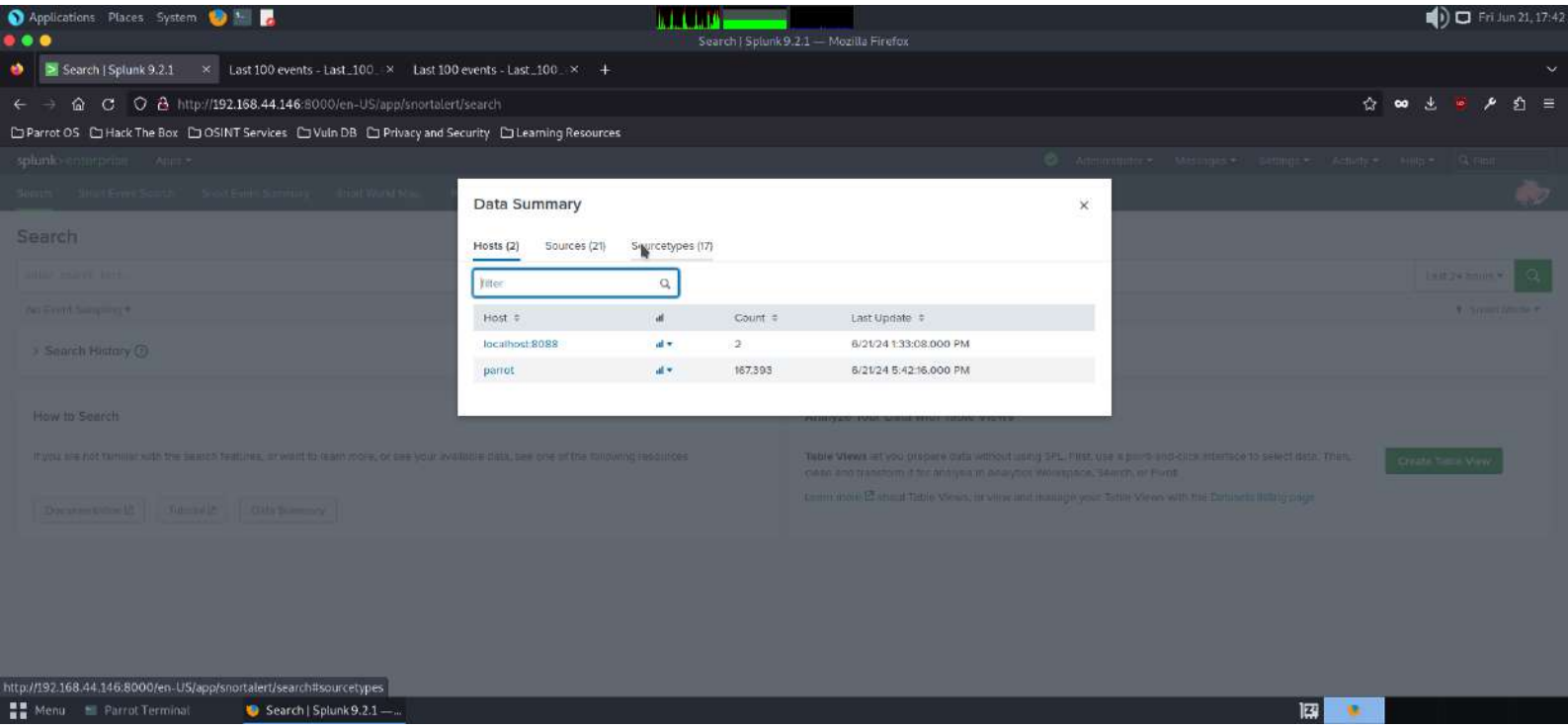

Applications Places System
Fri Jun 21, 17:53
Snort Event Search | Splunk 9.2.1 — Mozilla Firefox
Snort Event Search | Spl...
Snort Event Search - snort_...
http://192.168.44.146:8000/en-US/app/snortalert/snort_event_search?form.src_ip=*&form.src_port=*&form.dest_ip=*&form.dest_port=*&form.name=*
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
2024
_time
Top source IP in result set
192.168.17.217
192.168.61.48
192.168.61.105
192.168.17.250
192.168.17.153
Top destination IP in result set
192.168.44.135
192.168.17.217
192.168.17.147
Top alerts in result set
Event Name
SSH Connection Attempted
ICMP Message Detected
ATTACK_RESPONSES id check returned root
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
5.5
6
6.5
7
7.5
8
8.5
9
9.5
Alerts table of result set
Menu
Parrot Terminal
Snort Event Search | Spl...

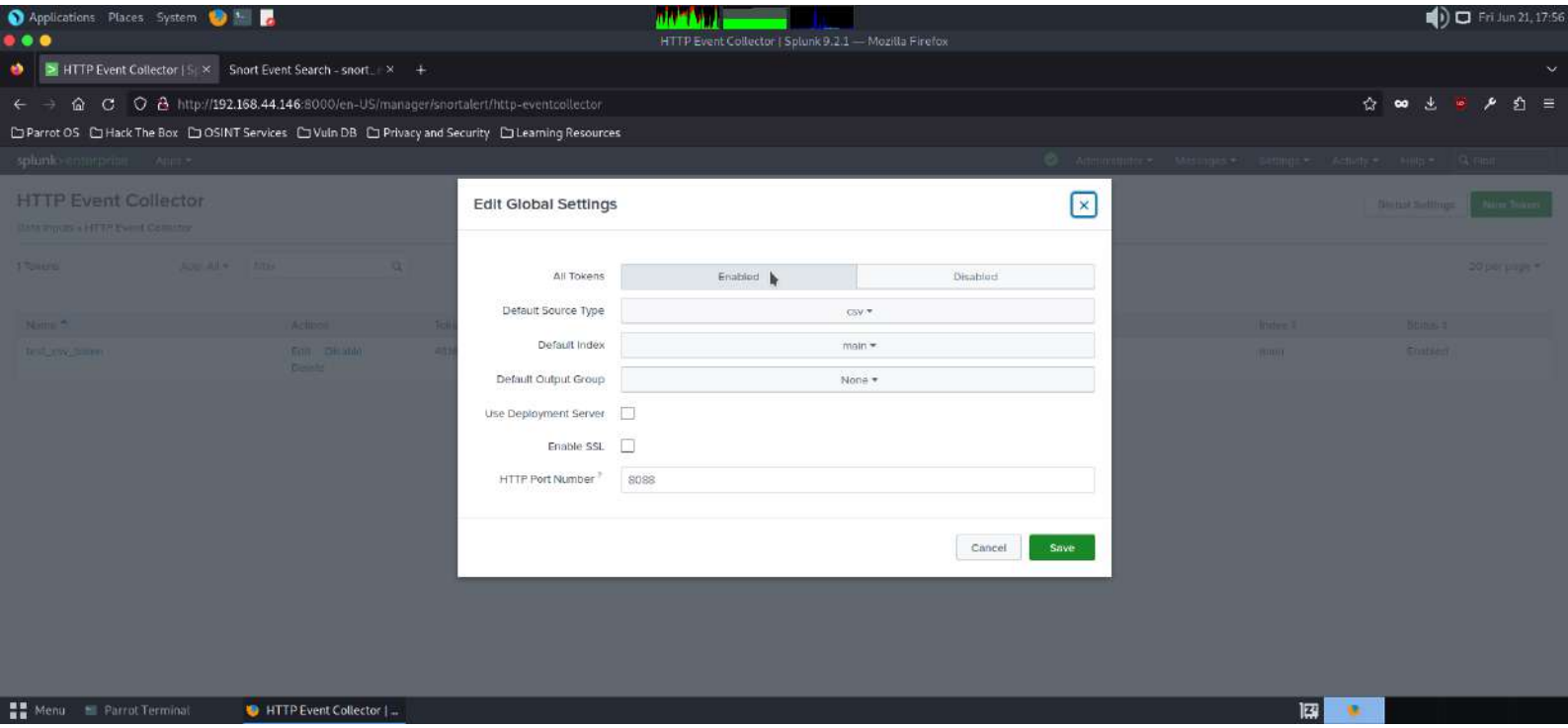

Applications Places System
Fri Jun 21, 17:53
Snort Event Search | Splunk 9.2.1 — Mozilla Firefox
Snort Event Search | Spl...
Snort Event Search - snort...
http://192.168.44.146:8000/en-US/app/snortalert/snort_event_search?form.src_ip=*&form.src_port=*&form.dest_ip=*&form.dest_port=*&form.name=*
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Source IP
Source Port
Destination IP
Destination Port
Protocol
Signature
Event Name
RAW
Time
192.168.17.217 53 192.168.17.147 60453 ICMP 100001 ICMP Message Detected
[**] [1:100001:1] ICMP Message Detected [**]
[Priority: 0]
05/29-12:04:33.890119 192.168.17.217 -> 192.168.17.147
ICMP TTL:64 TOS:0xC0 ID:35305 IpLen:20 DgmLen:153
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.17.147:53 -> 192.168.17.217:60453
UDP TTL:64 TOS:0x0 ID:57423 IpLen:20 DgmLen:125 DF
Len: 97 Csum: 63944
(97 more bytes of original packet)
** END OF DUMP
1716998673.690119
192.168.17.163 53 192.168.17.147 34355 ICMP 100001 ICMP Message Detected
[**] [1:100001:1] ICMP Message Detected [**]
[Priority: 0]
05/29-12:08:12.264525 192.168.17.163 -> 192.168.17.147
ICMP TTL:64 TOS:0xC0 ID:44899 IpLen:20 DgmLen:165
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.17.147:53 -> 192.168.17.163:34355
UDP TTL:64 TOS:0x0 ID:16903 IpLen:20 DgmLen:137 DF
Len: 109 Csum: 30951
(109 more bytes of original packet)
** END OF DUMP
1716998892.264525
192.168.17.163 53 192.168.17.147 34355 ICMP 100001 ICMP Message Detected
[**] [1:100001:1] ICMP Message Detected [**]
[Priority: 0]
05/29-12:03:12.264423 192.168.17.163 -> 192.168.17.147
ICMP TTL:64 TOS:0xC0 ID:44898 IpLen:20 DgmLen:153
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.17.147:53 -> 192.168.17.163:34355
UDP TTL:64 TOS:0x0 ID:16902 IpLen:20 DgmLen:125 DF
Len: 97 Csum: 31092
1716998592.264423
Menu
Parrot Terminal
Snort Event Search | Spl...

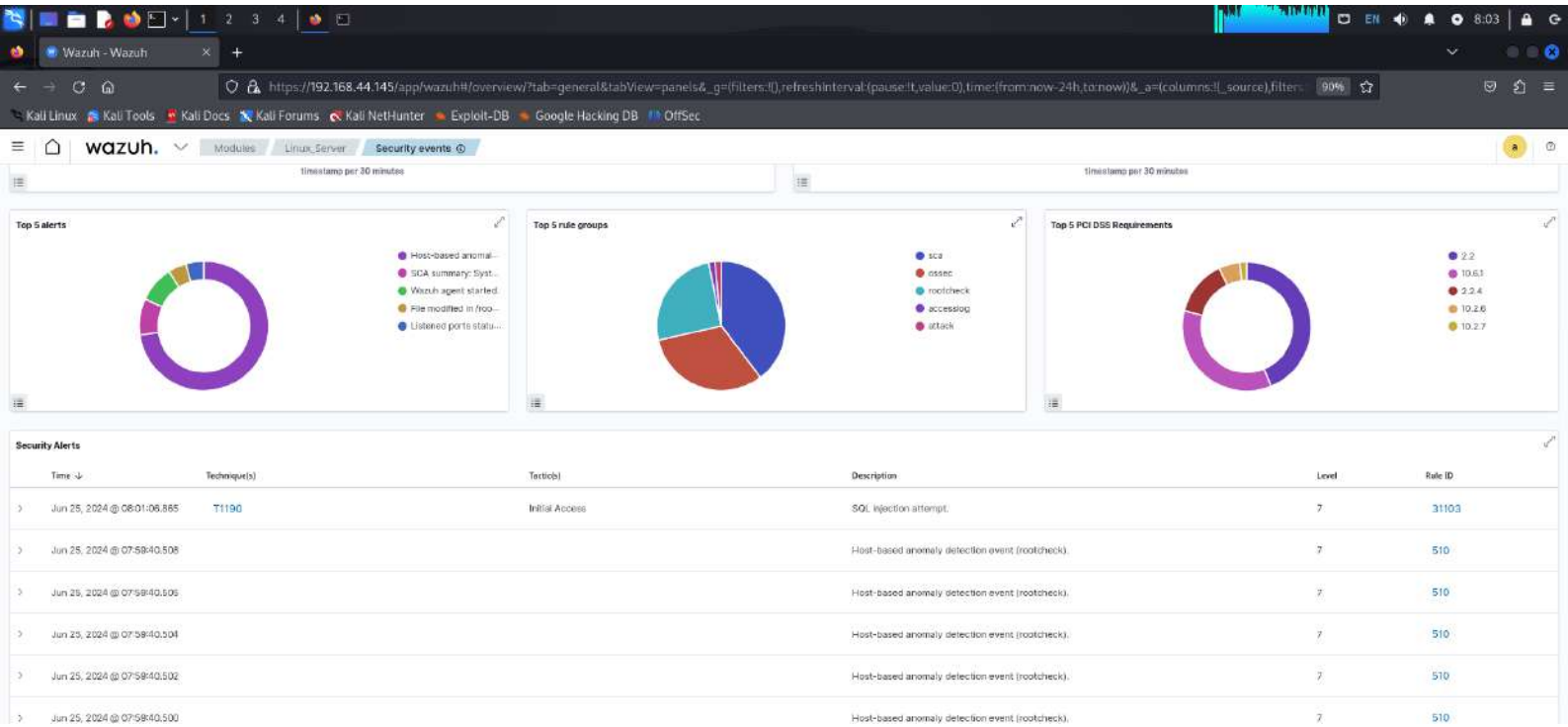

Applications Places System
Fri Jun 21, 17:42
Search | Splunk 9.2.1 — Mozilla Firefox
Search | Splunk 9.2.1
Last 100 events - Last_100...
Last 100 events - Last_100...
http://192.168.44.146:8000/en-US/app/snortalert/search
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Search
Search History
How to Search
Data Summary
Hosts (2)
Sources (21)
Sourcetypes (17)
filter
Source
Count
Last Update
/opt/splunk/var/log/splunk/splunkd-utility.log 23 6/21/24 5:33:55.000 PM
/opt/splunk/var/log/splunk/splunkd.log 16,144 6/21/24 5:42:36.000 PM
/opt/splunk/var/log/splunk/splunkd_access.log 2,079 6/21/24 5:42:28.000 PM
/opt/splunk/var/log/splunk/splunkd_stderr.log 1 6/21/24 5:34:32.000 PM
/opt/splunk/var/log/splunk/splunkd_ui_access.log 17,783 6/21/24 5:42:37.000 PM
/opt/splunk/var/log/splunk/web_access.log 148 6/21/24 5:40:05.000 PM
/opt/splunk/var/log/splunk/web_service.log 502 6/21/24 5:40:05.000 PM
snort 145 5/29/24 12:04:33.000 PM
token 2 6/21/24 1:33:08.000 PM
http://192.168.44.146:8000/en-US/app/snortalert/search#
Menu
Parrot Terminal
Search | Splunk 9.2.1 —...

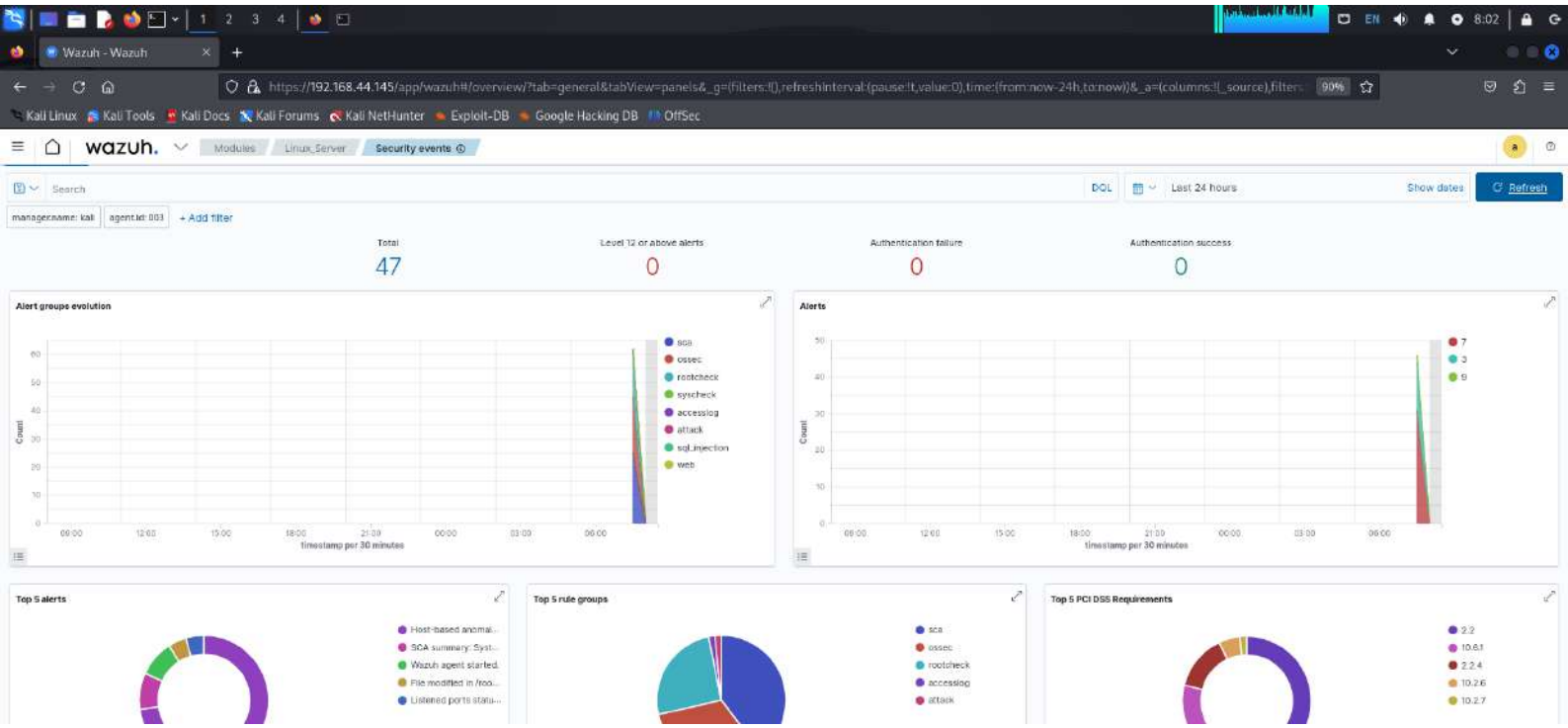

Applications Places System
Fri Jun 21, 18:02
Search | Splunk 9.2.1 — Mozilla Firefox
Search | Splunk 9.2.1
Snort Event Search - snort
http://192.168.44.146:8000/en-US/app/snortalert/search?q=search sourcetype%3Dcsv&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-24h%40h&latest=now&sid=
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Format Timeline
Zoom Out
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
index 1
linecount 1
punct 2
splunk_server 1
timestamp 1
Extract New Fields
6/21/24
1:33:08.000 PM
sourcetype,test,trail
Event Actions
Type
Field
Value
Actions
Selected
host
localhost:8088
source
token
sourcetype
csv
Event
timestamp
none
Time
_time
2024-06-21T13:33:08.000-04:00
Default
index
main
linecount
1
punct
splunk_server
parrot
6/21/24
1:31:28.000 PM
{ [-]
event: hello world
}
Show as raw text
host = localhost:8088
source = token
sourcetype = csv
Menu
Parrot Terminal
Search | Splunk 9.2.1 —...
Parrot Terminal

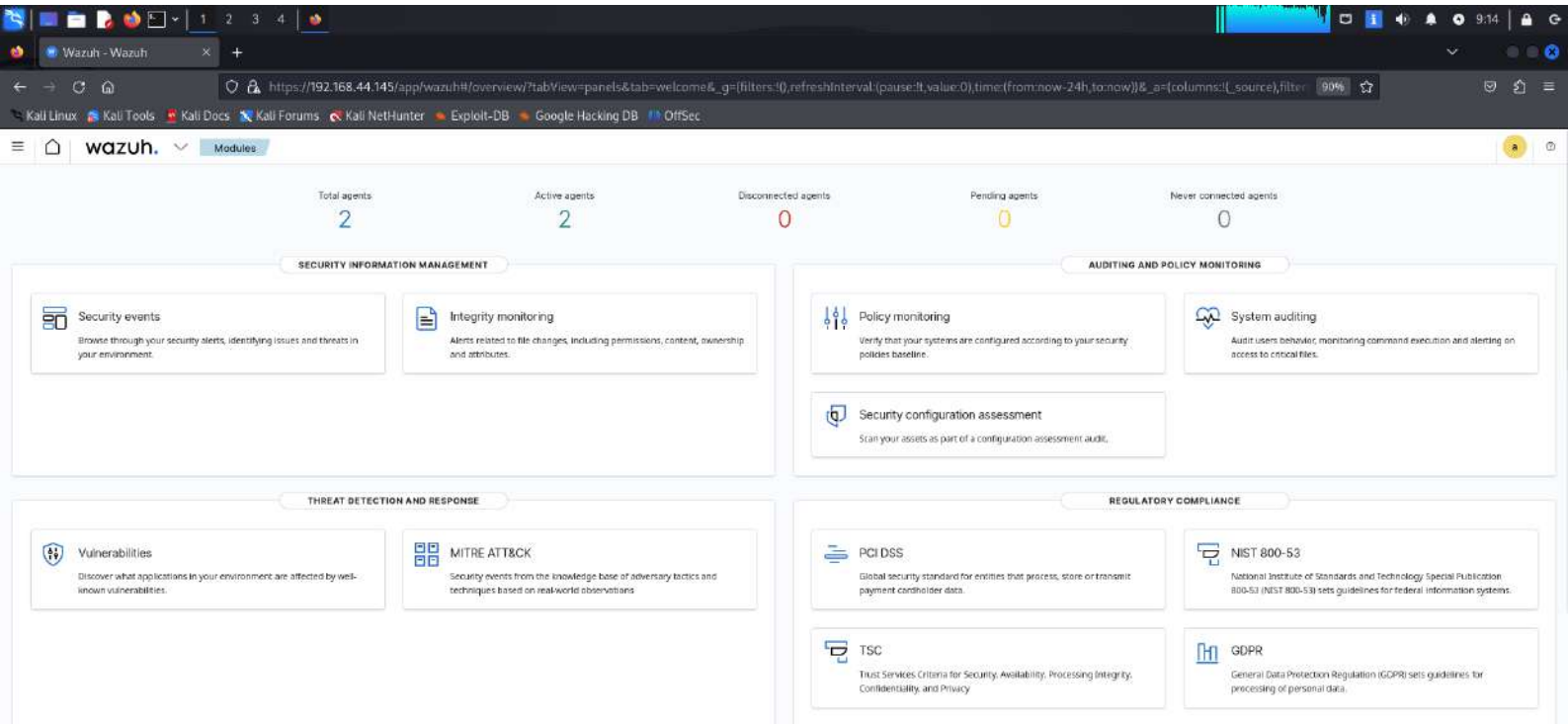

Applications Places System
Fri Jun 21, 17:55
HTTP Event Collector | Splunk 9.2.1 — Mozilla Firefox
HTTP Event Collector | S
Snort Event Search - snort
http://192.168.44.146:8000/en-US/manager/snortalert/http-eventcollector
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
HTTP Event Collector
Data Inputs » HTTP Event Collector
Global Settings
New Token
1 Tokens
App: All
filter
20 per page
Name
Actions
Token Value
Source Type
Index
Status
test_csv_token
Edit
Disable
Delete
48164b27-04c0-4783-9921-13f4b25882cd
main
Enabled
Menu
Parrot Terminal
HTTP Event Collector | ...

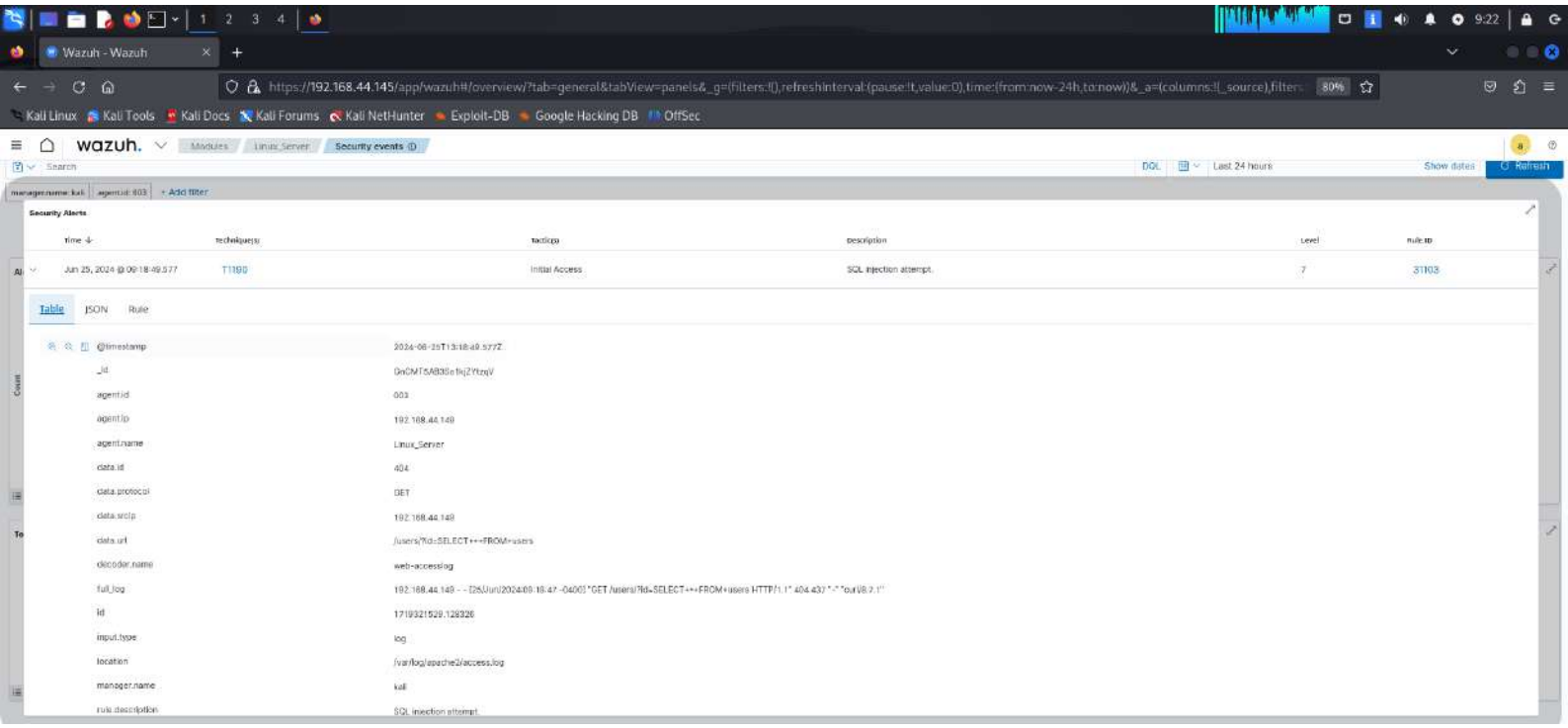

Applications Places System
Fri Jun 21, 17:42
Search | Splunk 9.2.1 — Mozilla Firefox
Search | Splunk 9.2.1
Last 100 events - Last_100...
Last 100 events - Last_100...
http://192.168.44.146:8000/en-US/app/snortalert/search
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Data Summary
Hosts (2)
Sources (21)
Sourcetypes (17)
filter
Host
Count
Last Update
localhost:8088
2
6/21/24 1:33:08.000 PM
parrot
167,393
6/21/24 5:42:16.000 PM
Search
Search History
How to Search
Create Table View
http://192.168.44.146:8000/en-US/app/snortalert/search#sourcetypes
Menu
Parrot Terminal
Search | Splunk 9.2.1 —...

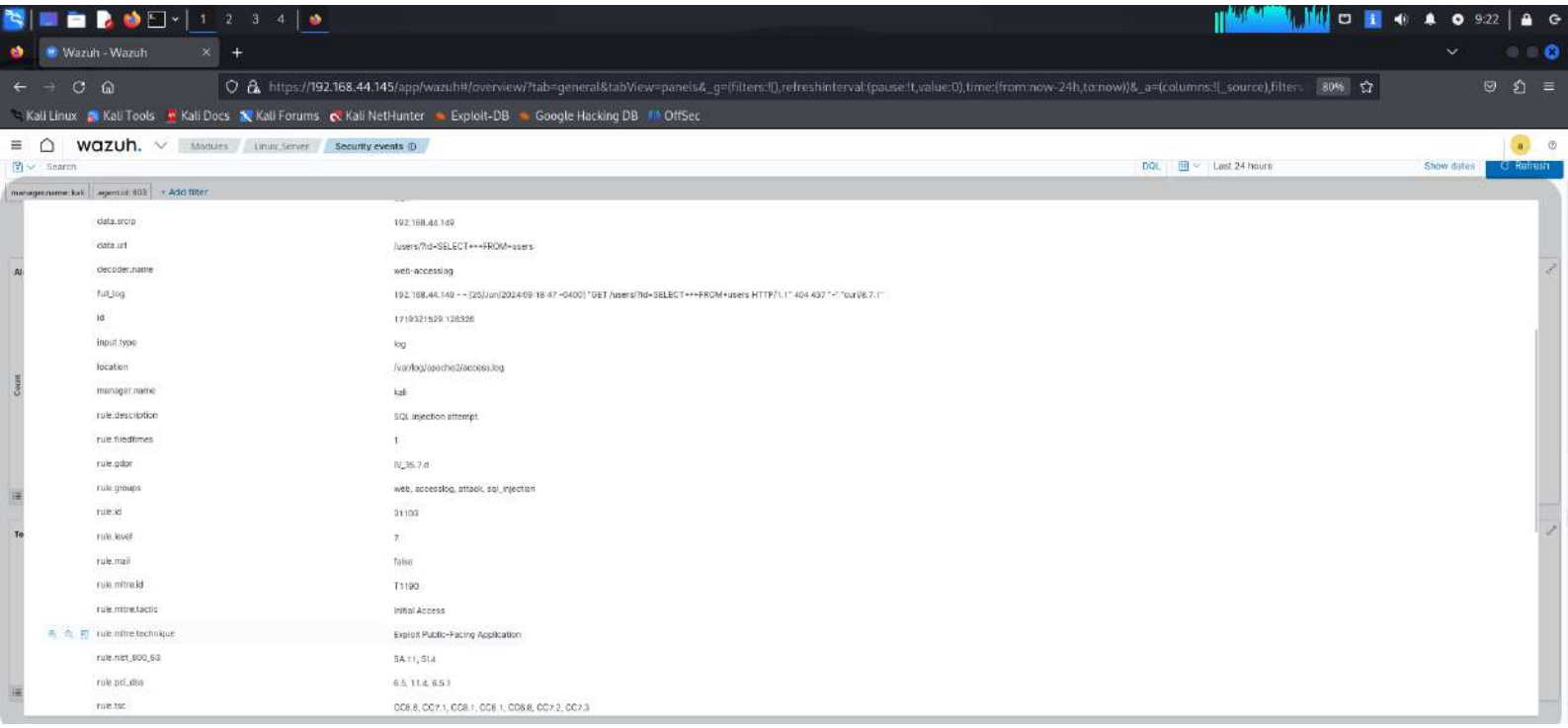

Applications Places System
Fri Jun 21, 17:56
HTTP Event Collector | Splunk 9.2.1 — Mozilla Firefox
HTTP Event Collector | S
Snort Event Search - snort
http://192.168.44.146:8000/en-US/manager/snortalert/http-eventcollector
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
HTTP Event Collector
Edit Global Settings
All Tokens
Enabled
Disabled
Default Source Type
csv
Default Index
main
Default Output Group
None
Use Deployment Server
Enable SSL
HTTP Port Number
8088
Cancel
Save
Menu
Parrot Terminal
HTTP Event Collector | ...

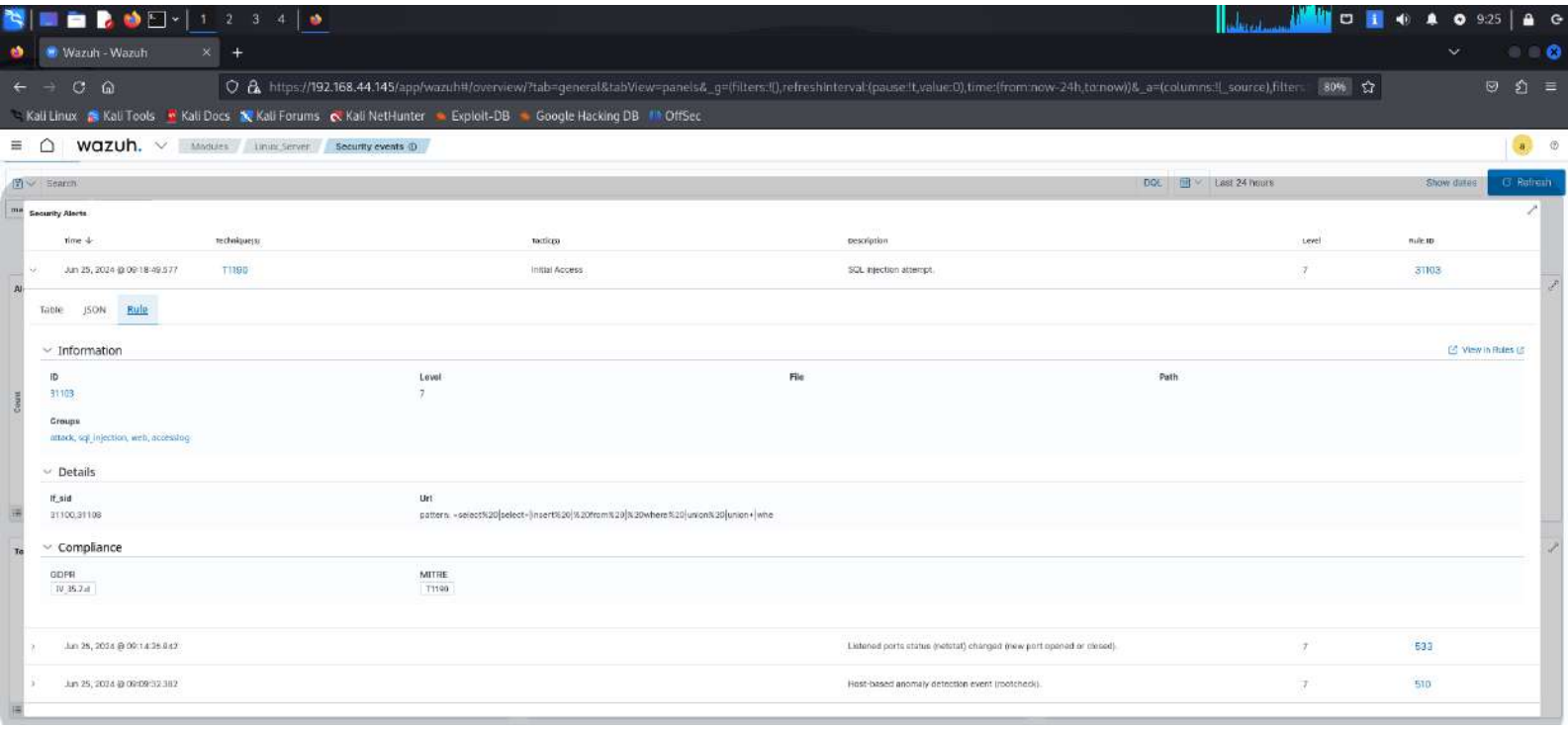

Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Linux_Server
Security events
timestamp per 30 minutes
timestamp per 30 minutes
Top 5 alerts
Host-based anomal...
SCA summary: Syst...
Wazuh agent started.
File modified in /roo...
Listened ports statu...
Top 5 rule groups
sca
ossec
rootcheck
accesslog
attack
Top 5 PCI DSS Requirements
2.2
10.6.1
2.2.4
10.2.6
10.2.7
Security Alerts
Time
Technique(s)
Tactic(s)
Description
Level
Rule ID
Jun 25, 2024 @ 08:01:06.865
T1190
Initial Access
SQL injection attempt.
7
31103
Jun 25, 2024 @ 07:59:40.508
Host-based anomaly detection event (rootcheck).
7
510
Jun 25, 2024 @ 07:59:40.505
Host-based anomaly detection event (rootcheck).
7
510
Jun 25, 2024 @ 07:59:40.504
Host-based anomaly detection event (rootcheck).
7
510
Jun 25, 2024 @ 07:59:40.502
Host-based anomaly detection event (rootcheck).
7
510
Jun 25, 2024 @ 07:59:40.500
Host-based anomaly detection event (rootcheck).
7
510

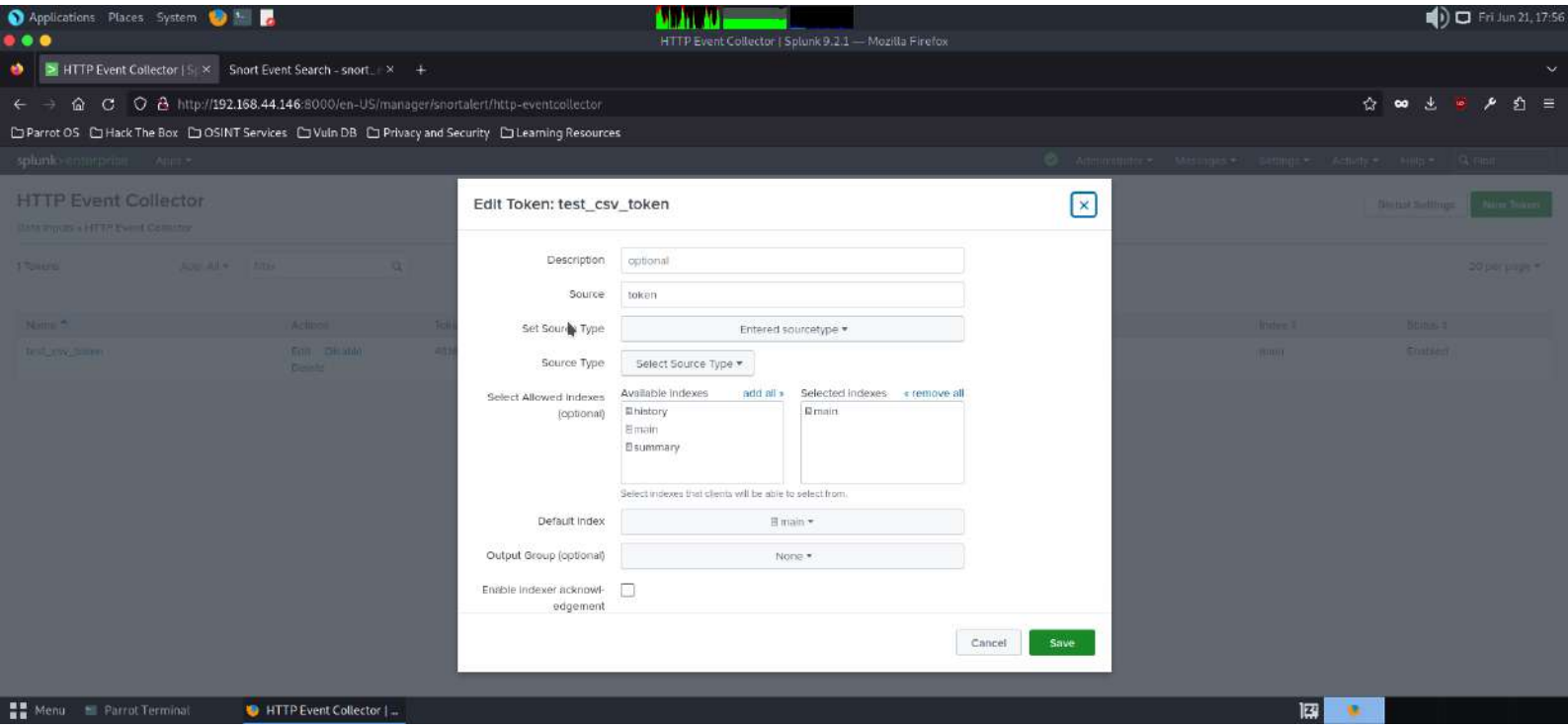

Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Linux_Server
Security events
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: kali
agent.id: 003
+ Add filter
Total
47
Level 12 or above alerts
0
Authentication failure
0
Authentication success
0
Alert groups evolution
sca
ossec
rootcheck
syscheck
accesslog
attack
sql_injection
web
Count
timestamp per 30 minutes
Alerts
7
3
9
Count
timestamp per 30 minutes
Top 5 alerts
Host-based anomal...
SOA summary: Syst...
Wazuh agent started.
File modified in /roo...
Listened ports statu...
Top 5 rule groups
sca
ossec
rootcheck
accesslog
attack
Top 5 PCI DSS Requirements
2.2
10.6.1
2.2.4
10.2.6
10.2.7


Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tabView=panels&tab=welcome&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filter
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Total agents
2
Active agents
2
Disconnected agents
0
Pending agents
0
Never connected agents
0
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.
THREAT DETECTION AND RESPONSE
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations
REGULATORY COMPLIANCE
PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.
TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

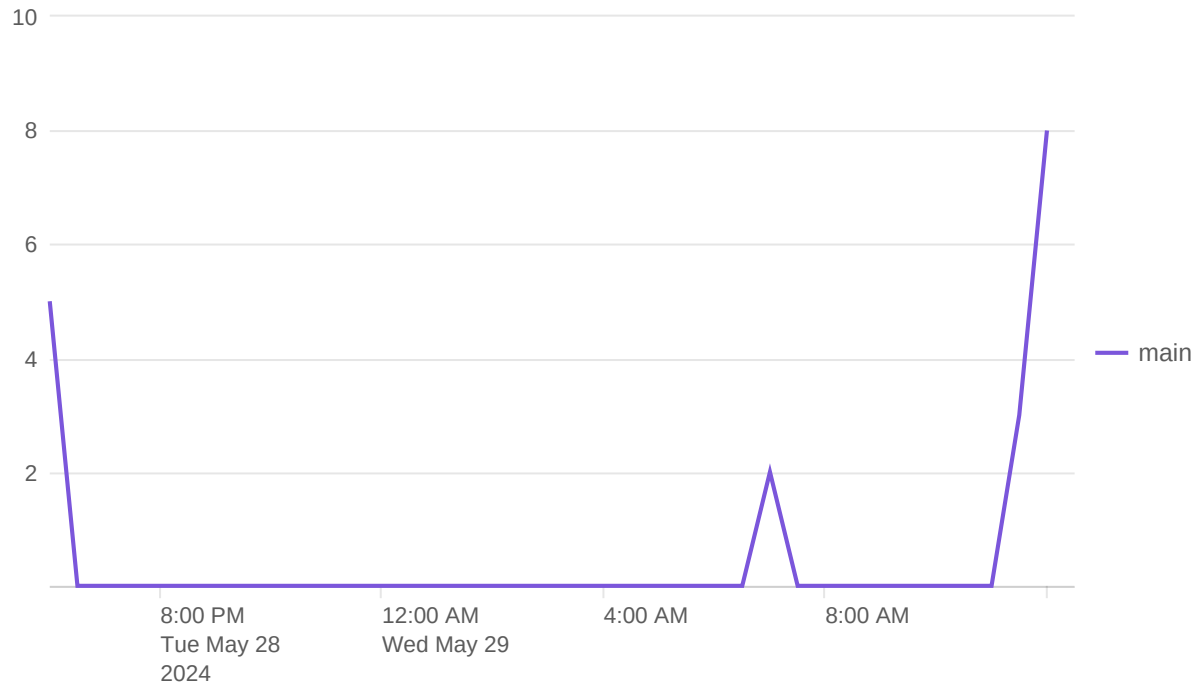

Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Linux_Server
Security events
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: kali
agent.id: 003
+ Add filter
Security Alerts
time
technique(s)
tactic(s)
description
level
rule.id
Jun 25, 2024 @ 09:18:49.577
T1190
Initial Access
SQL injection attempt.
7
31103
Table
JSON
Rule
@timestamp
2024-06-25T13:18:49.577Z
_id
GnCMT5AB3Se1kjZYtzqV
agent.id
003
agent.ip
192.168.44.149
agent.name
Linux_Server
data.id
404
data.protocol
GET
data.srcip
192.168.44.149
data.url
/users/?id=SELECT+++FROM+users
decoder.name
web-accesslog
full_log
192.168.44.149 - - [25/Jun/2024:09:18:47 -0400] "GET /users/?id=SELECT+++FROM+users HTTP/1.1" 404 437 "-" "curl/8.7.1"
id
1719321529.129326
input.type
log
location
/var/log/apache2/access.log
manager.name
kali
rule.description
SQL injection attempt


Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Linux_Server
Security events
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: kali
agent.id: 003
+ Add filter
data.srcip 192.168.44.149
data.url /users/?id=SELECT+++FROM+users
decoder.name web-accesslog
full_log 192.168.44.149 - - [25/Jun/2024:09:18:47 -0400] "GET /users/?id=SELECT+++FROM+users HTTP/1.1" 404 437 "-" "curl/8.7.1"
id 1719321529.128326
input.type log
location /var/log/apache2/access.log
manager.name kali
rule.description SQL injection attempt
rule.firedtimes 1
rule.gdpr IV_35.7.d
rule.groups web, accesslog, attack, sql_injection
rule.id 31103
rule.level 7
rule.mail false
rule.mitre.id T1190
rule.mitre.tactic Initial Access
rule.mitre.technique Exploit Public-Facing Application
rule.nist_800_53 SA.11, SI.4
rule.pci_dss 6.5, 11.4, 6.5.1
rule.tsc CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3

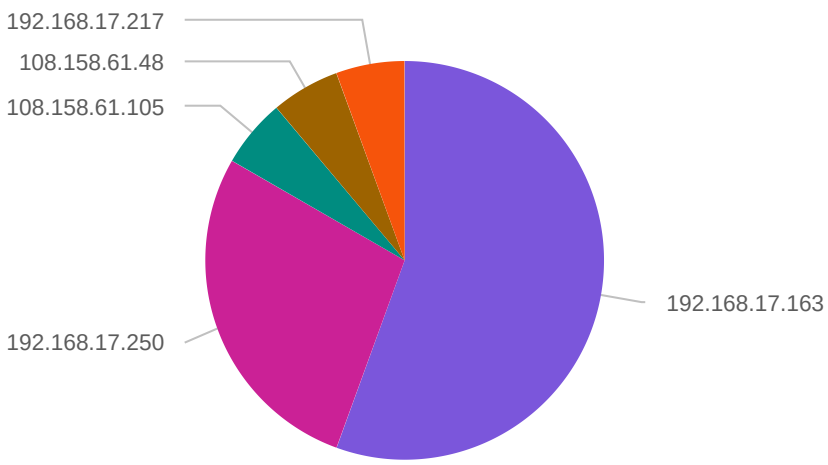

Wazuh - Wazuh
https://192.168.44.145/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
wazuh.
Modules
Linux_Server
Security events
Search
DQL
Last 24 hours
Show dates
Refresh
Security Alerts
time
technique(s)
tactic(s)
description
level
rule.id
Jun 25, 2024 @ 09:18:49.577
T1190
Initial Access
SQL injection attempt.
7
31103
Table
JSON
Rule
Information
View in Rules
ID
31103
Level
7
File
Path
Groups
attack, sql_injection, web, accesslog
Details
If_sid
31100,31108
Url
pattern: =select%20|select+|insert%20|%20from%20|%20where%20|union%20|union+|whe
Compliance
GDPR
IV_35.7.d
MITRE
T1190
Jun 25, 2024 @ 09:14:35.843
Listened ports status (netstat) changed (new port opened or closed).
7
533
Jun 25, 2024 @ 09:09:52.382
Host-based anomaly detection event (rootcheck).
7
510


Applications Places System
Fri Jun 21, 17:56
HTTP Event Collector | Splunk 9.2.1 — Mozilla Firefox
HTTP Event Collector | S
Snort Event Search - snort
http://192.168.44.146:8000/en-US/manager/snortalert/http-eventcollector
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
HTTP Event Collector
Edit Token: test_csv_token
Description
optional
Source
token
Set Source Type
Entered sourcetype
Source Type
Select Source Type
Select Allowed Indexes (optional)
Available indexes
add all »
history
main
summary
Selected indexes
« remove all
main
Select indexes that clients will be able to select from.
Default Index
main
Output Group (optional)
None
Enable indexer acknowledgement
Cancel
Save
Menu
Parrot Terminal
HTTP Event Collector | ...

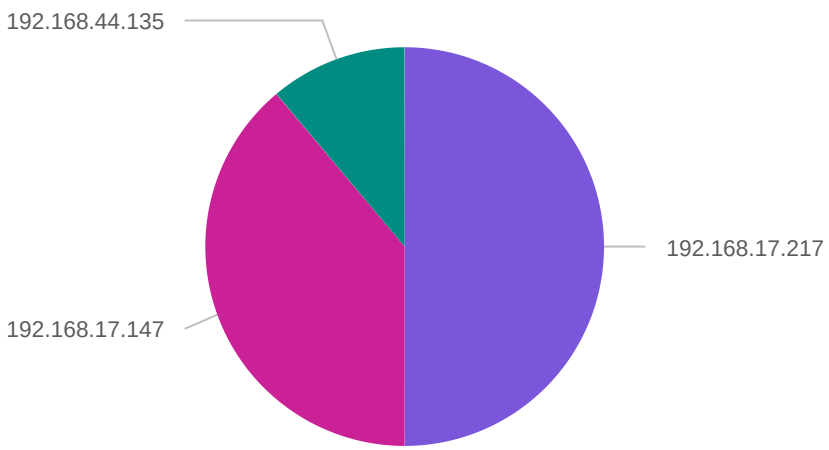
Events by time in result set



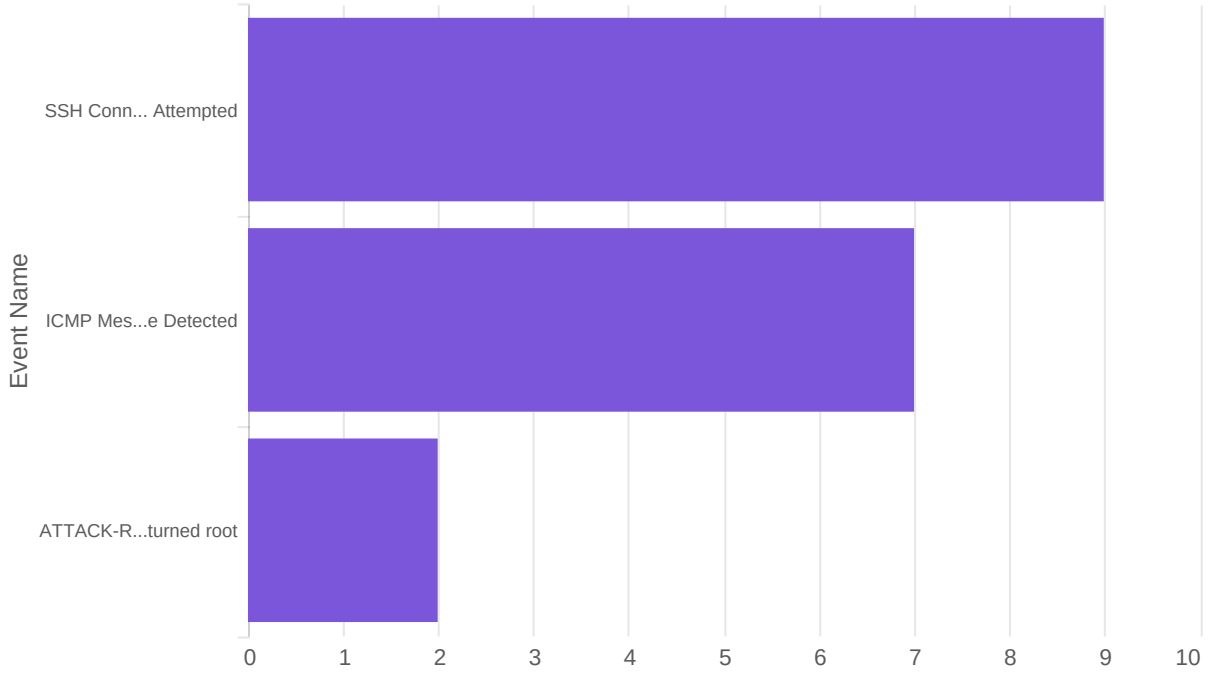
Top source IP in result set



Top destination IP in result set



Top alerts in result set



Alerts table of result set

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
192.168.17.217	53	192.168.17.147	60453	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:04:33.090119 192.168.17.217 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:35305 IpLen:20 DgmLen:153 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.217:60453 UDP TTL:64 TOS:0x0 ID: 57423 IpLen:20 DgmLen: 125 DF Len: 97 Csum: 63944 (97 more bytes of original packet) ** END OF DUMP	1716998673.090119
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264525 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44699 IpLen:20 DgmLen:165 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16903 IpLen:20 DgmLen: 137 DF Len: 109 Csum: 30551 (109 more bytes of original packet) ** END OF DUMP	1716998592.264525

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264423 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44698 IpLen:20 DgmLen:153 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16902 IpLen:20 DgmLen: 125 DF Len: 97 Csum: 31092 (97 more bytes of original packet) ** END OF DUMP	1716998592.264423
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264422 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44697 IpLen:20 DgmLen:165 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16901 IpLen:20 DgmLen: 137 DF Len: 109 Csum: 30551 (109 more bytes of original packet) ** END OF DUMP	1716998592.264422
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264422 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44696 IpLen:20 DgmLen:153 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16900 IpLen:20 DgmLen: 125 DF Len: 97 Csum: 31092 (97 more bytes of original packet) ** END OF DUMP	1716998592.264422

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264422 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44695 IpLen:20 DgmLen:165 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16899 IpLen:20 DgmLen: 137 DF Len: 109 Csum: 30551 (109 more bytes of original packet) ** END OF DUMP	1716998592.264422
192.168.17.163	53	192.168.17.147	34355	ICMP	100001	ICMP Message Detected	[**] [1:100001:1] ICMP Message Detected [**] [Priority: 0] 05/29-12:03:12.264017 192.168.17.163 -> 192 .168.17.147 ICMP TTL:64 TOS:0xC0 ID:44694 IpLen:20 DgmLen:153 Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE ** ORIGINAL DATAGRAM DUMP: 192.168.17.147:53 -> 192.168.17.163:34355 UDP TTL:64 TOS:0x0 ID: 16898 IpLen:20 DgmLen: 125 DF Len: 97 Csum: 31092 (97 more bytes of original packet) ** END OF DUMP	1716998592.264017
192.168.17.163	36060	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] 05/29-12:03:01.191294 192.168.17.163:36060 - > 192.168.17.217:22 TCP TTL:64 TOS:0x10 ID :8075 IpLen:20 DgmLen: 60 DF ******S* Seq: 0xCE9F15C4 Ack: 0x0 Win: 0x7D78 TcpLen: 40 TCP Options (5) => MSS: 1460 SackOK TS: 2458129316 0 NOP WS: 7	1716998581.191294

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
192.168.17.163	59209	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] 05/29-11:45:50.656422 192.168.17.163:59209 -> 192.168.17.217:22 TCP TTL:47 TOS:0x0 ID: 30890 IpLen:20 DgmLen: 44 ******S* Seq: 0xDD4A8ECA Ack: 0x0 Win: 0x400 TcpLen: 24 TCP Options (1) => MSS: 1460	1716997550.656422
192.168.17.163	40144	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] 05/29-11:45:18.336310 192.168.17.163:40144 -> 192.168.17.217:22 TCP TTL:64 TOS:0x10 ID :25375 IpLen:20 DgmLen: 60 DF ******S* Seq: 0x89B884D6 Ack: 0x0 Win: 0x7D78 TcpLen: 40 TCP Options (5) => MSS: 1460 SackOK TS: 2457066590 0 NOP WS: 7	1716997518.336310
192.168.17.163	54240	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:2] SSH Connection Attempted [**] [Priority: 0] 05/29-11:45:08.834242 192.168.17.163:54240 -> 192.168.17.217:22 TCP TTL:64 TOS:0x10 ID :14599 IpLen:20 DgmLen: 60 DF ******S* Seq: 0xCD30D333 Ack: 0x0 Win: 0x7D78 TcpLen: 40 TCP Options (5) => MSS: 1460 SackOK TS: 2457057087 0 NOP WS: 7	1716997508.834242
108.158.61.105	80	192.168.44.135	41204	TCP	498	ATTACK-RESPONSES id check returned root	[**] [1:498:6] ATTACK-RESPONSES id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] 05/29-07:02:18.730020 108.158.61.105:80 -> 192.168.44.135:41204 TCP TTL:128 TOS:0x0 ID :7942 IpLen:20 DgmLen: 575 ***AP*** Seq: 0x210C57FE Ack: 0x8003D95E Win: 0xFAF0 TcpLen: 20	1716980538.730020

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
108.158.61.48	80	192.168.44.135	58220	TCP	498	ATTACK-RESPONSES id check returned root	[**] [1:498:6] ATTACK-RESPONSES id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] 05/29-07:01:00.825268 108.158.61.48:80 -> 192.168.44.135:58220 TCP TTL:128 TOS:0x0 ID :7605 IpLen:20 DgmLen: 573 ***AP*** Seq: 0x29913FA9 Ack: 0xA329FE9D Win: 0xFAF0 TcpLen: 20	1716980460.825268
192.168.17.250	53787	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:1] SSH Connection Attempted [**] [Priority: 0] 05/28-18:21:47.680976 192.168.17.250:53787 -> 192.168.17.217:22 TCP TTL:128 TOS:0x0 ID :10973 IpLen:20 DgmLen: 52 DF ******S* Seq: 0xC8B0E3D2 Ack: 0x0 Win: 0xFAF0 TcpLen: 32 TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK	1716934907.680976
192.168.17.250	53787	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:1] SSH Connection Attempted [**] [Priority: 0] 05/28-18:21:47.167973 192.168.17.250:53787 -> 192.168.17.217:22 TCP TTL:128 TOS:0x0 ID :10972 IpLen:20 DgmLen: 52 DF ******S* Seq: 0xC8B0E3D2 Ack: 0x0 Win: 0xFAF0 TcpLen: 32 TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK	1716934907.167973
192.168.17.250	53787	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:1] SSH Connection Attempted [**] [Priority: 0] 05/28-18:21:46.656007 192.168.17.250:53787 -> 192.168.17.217:22 TCP TTL:128 TOS:0x0 ID :10971 IpLen:20 DgmLen: 52 DF ******S* Seq: 0xC8B0E3D2 Ack: 0x0 Win: 0xFAF0 TcpLen: 32 TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK	1716934906.656007

Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature	Event Name	RAW	Time
192.168.17.250	53787	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:1] SSH Connection Attempted [**] [Priority: 0] 05/28-18:21:46.144405 192.168.17.250:53787 -> 192.168.17.217:22 TCP TTL:128 TOS:0x0 ID :10970 IpLen:20 DgmLen: 52 DF ******S* Seq: 0xC8B0E3D2 Ack: 0x0 Win: 0xFAF0 TcpLen: 32 TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK	1716934906.144405
192.168.17.250	53787	192.168.17.217	22	TCP	100002	SSH Connection Attempted	[**] [1:100002:1] SSH Connection Attempted [**] [Priority: 0] 05/28-18:21:45.628807 192.168.17.250:53787 -> 192.168.17.217:22 TCP TTL:128 TOS:0x0 ID :10969 IpLen:20 DgmLen: 52 DF ******S* Seq: 0xC8B0E3D2 Ack: 0x0 Win: 0xFAF0 TcpLen: 32 TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK	1716934905.628807

Last 100 events

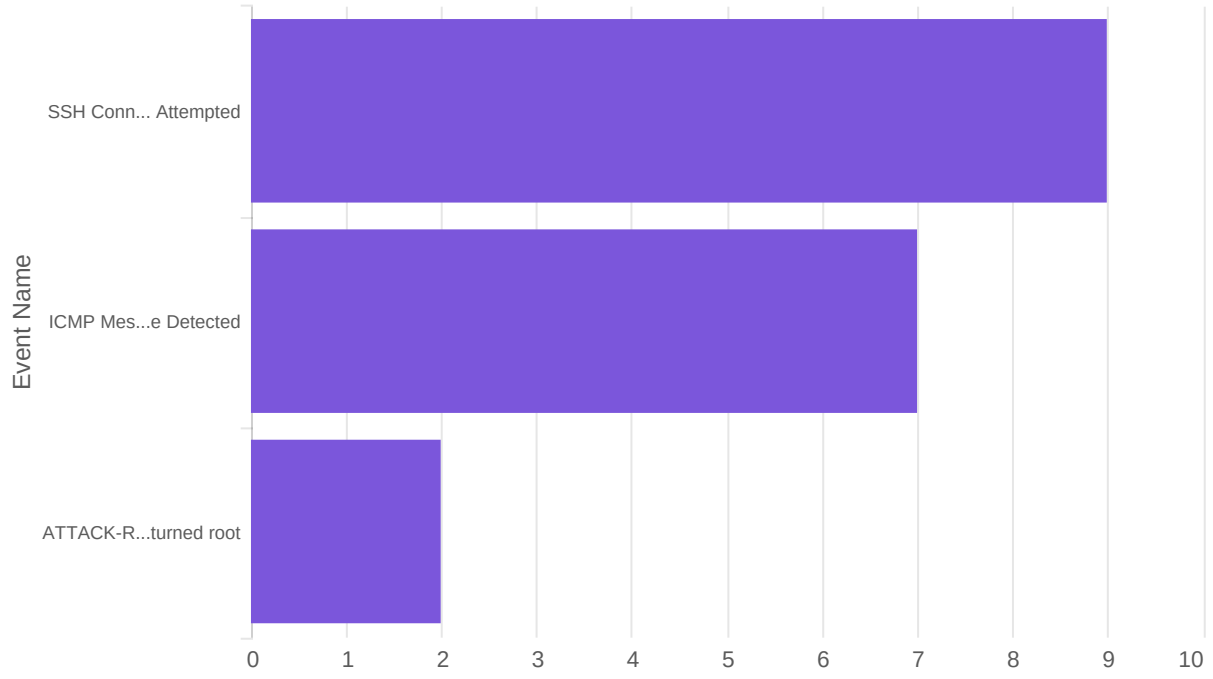
#	Time	Source Host	Source IP	Source Country	Destination IP	Destination Country	Signature	Event Name
1	1716998673.090119	192.168.17.217	192.168.17.217	-	192.168.17.147	-	100001	ICMP Message Detected
2	1716998592.264525	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
3	1716998592.264423	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
4	1716998592.264422	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
5	1716998592.264422	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
6	1716998592.264422	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
7	1716998592.264017	192.168.17.163	192.168.17.163	-	192.168.17.147	-	100001	ICMP Message Detected
8	1716998581.191294	192.168.17.163	192.168.17.163	-	192.168.17.217	-	100002	SSH Connection Attempted
9	1716997550.656422	192.168.17.163	192.168.17.163	-	192.168.17.217	-	100002	SSH Connection Attempted
10	1716997518.336310	192.168.17.163	192.168.17.163	-	192.168.17.217	-	100002	SSH Connection Attempted
11	1716997508.834242	192.168.17.163	192.168.17.163	-	192.168.17.217	-	100002	SSH Connection Attempted
12	1716980538.730020	server-108-158-61-105.bom78.r.cloudfront.net	108.158.61.105	India	192.168.44.135	India	498	ATTACK-RESPONSES id check returned root
13	1716980460.825268	server-108-158-61-48.bom78.r.cloudfront.net	108.158.61.48	India	192.168.44.135	India	498	ATTACK-RESPONSES id check returned root
14	1716934907.680976	192.168.17.250	192.168.17.250	-	192.168.17.217	-	100002	SSH Connection Attempted
15	1716934907.167973	192.168.17.250	192.168.17.250	-	192.168.17.217	-	100002	SSH Connection Attempted
16	1716934906.656007	192.168.17.250	192.168.17.250	-	192.168.17.217	-	100002	SSH Connection Attempted

#	Time	Source Host	Source IP	Source Country	Destination IP	Destination Country	Signature	Event Name
17	1716934906.144405	192.168.17.250	192.168.17.250	-	192.168.17.217	-	100002	SSH Connection Attempted
18	1716934905.628807	192.168.17.250	192.168.17.250	-	192.168.17.217	-	100002	SSH Connection Attempted

Alerts table of result set

Time	Event
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	
None	

Top alerts in result set



Event Name	count
SSH Connection Attempted	9
ICMP Message Detected	7
ATTACK-RESPONSES id check returned root	2