AlienVault: Threat Hunting/Network Analysis

November 18, 2020 By Raj Chandel

What is threat hunting?

The process of threat hunting involves proactively searching for malware or attackers that are hiding within a network. Rather than simply relying on security solutions or services to detect threats, threat hunting is a predictive element to a layered security strategy, empowering organizations to go on the offensive looking for threats. Threat hunting is typically carried out by highly skilled security professionals using sophisticated toolsets to identify and stop hard-to-find malicious activities on a network.

According to **Microsoft**, an attacker resides on a compromised network a median time of 146 days before being discovered, making this kind of attack an **Advanced Persistent Threat (APT)**. In this amount of time, attackers residing on a network in stealth can exfiltrate data, access applications to identify and use business details to commit fraud, or laterally move through a network gathering credentials for access to even more valuable data and resources.

Table of Content

- Prerequisites
- Credentials
- Why is Threat Hunting necessary?
- Brute force detection via a different protocol
- Alerts Attack based Tickets
- Traffic Analysis
- Deployment Status
- OTX: Open Threat Exchange
- Indicators of compromise (IoCs)

Prerequisites

- Kali (Attacker Machine)
- Ubuntu 20.04.1
- Putty (for log-in in servers via different protocols)
- Root privileges

Credentials

- AlienVault IP: – 192.168.1.70
- Ubuntu Machine IP: – 192.168.1.9
- Kali (Attacker Machine IP): – 192.168.1.12Why is threat hunting necessary?

- A layered security strategy can be effective in stopping the majority of cyberattacks. However, it should be assumed that some small percentage of advanced attacks will evade detection by traditional security solutions, giving cybercriminals access to an organization’s network for as long as they deem necessary to carry out their malicious activities.
- Implementing a security posture that prevents and detects attacks is defensive– as the idea is to attempt to stop an attack before it happens.
- Threat hunting is a predictive and offensive tactic, based on the assumption that an attacker has already successfully gained access (despite an organization’s best efforts).
- Threat hunting uses a mixture of forensics capabilities and threat intelligence to track down where attackers have established footholds within the network and eliminate their access before any damaging malicious actions can take place.

Brute Force detection via different protocols

Brute Force simply can be defined as attempting to log-in without knowing the username or password.

This type can be evaded or avoided by using Brute force Detection by using different type of SIEM tools such as AlienVault

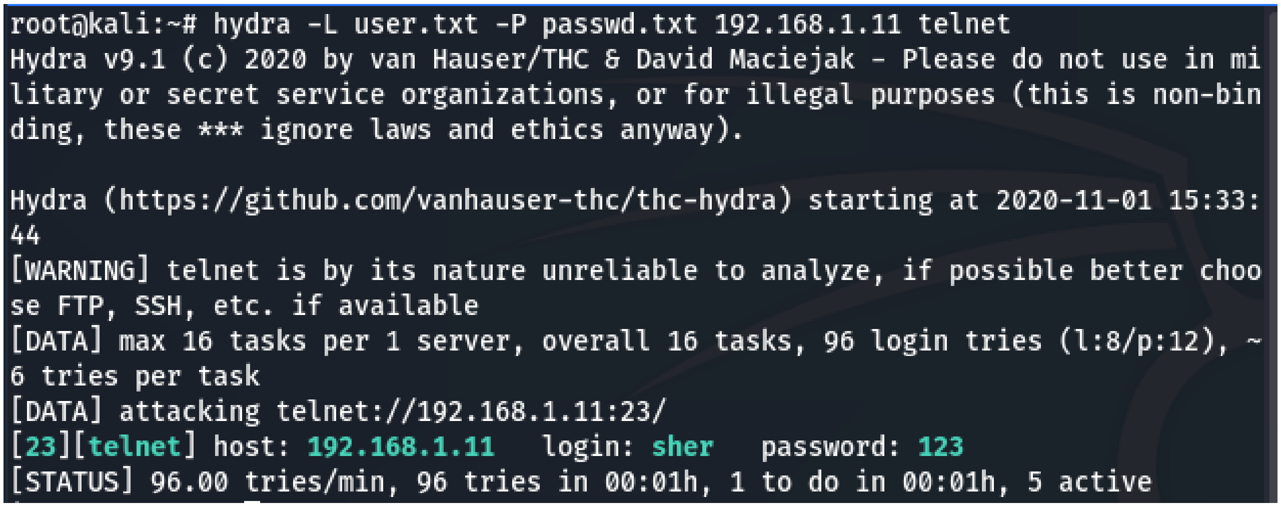
Without of much theory Lets get started with the detection scenario

Let’s take a look ?!!

We are going to perform Brute Force via different protocols

To perform Telnet based Brute Force fire up your KALI machine and run the following command:

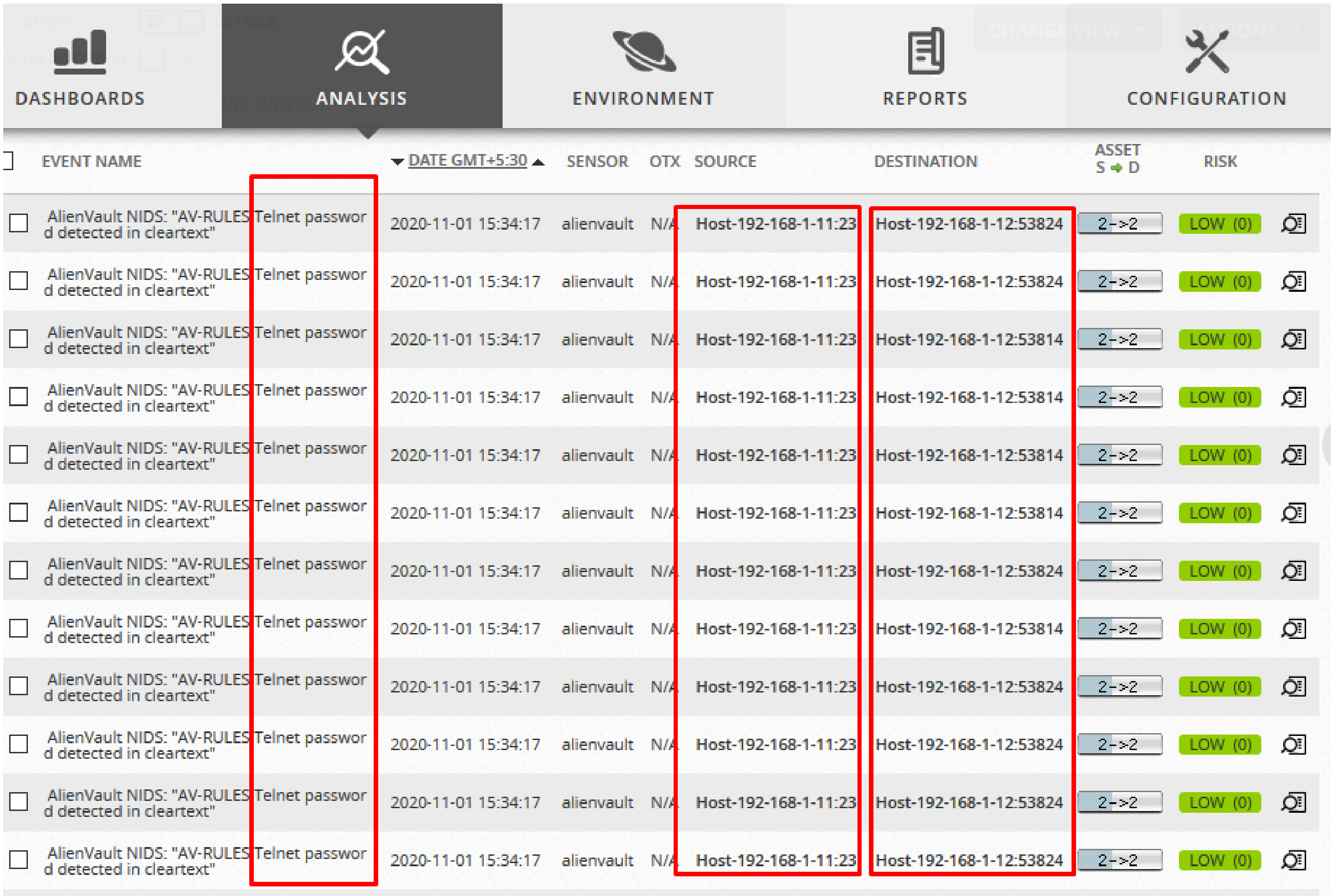
```
hydra -L user.txt -P passwd.txt 192.168.1.11 telnet
```



```
root@kali:~# hydra -L user.txt -P passwd.txt 192.168.1.11 telnet
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-01 15:33:
44
[WARNING] telnet is by its nature unreliable to analyze, if possible better choo
se FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 96 login tries (l:8/p:12), ~
6 tries per task
[DATA] attacking telnet://192.168.1.11:23/
[23][telnet] host: 192.168.1.11   login: sher   password: 123
[STATUS] 96.00 tries/min, 96 tries in 00:01h, 1 to do in 00:01h, 5 active
```

Let’s see the Magic ?!!

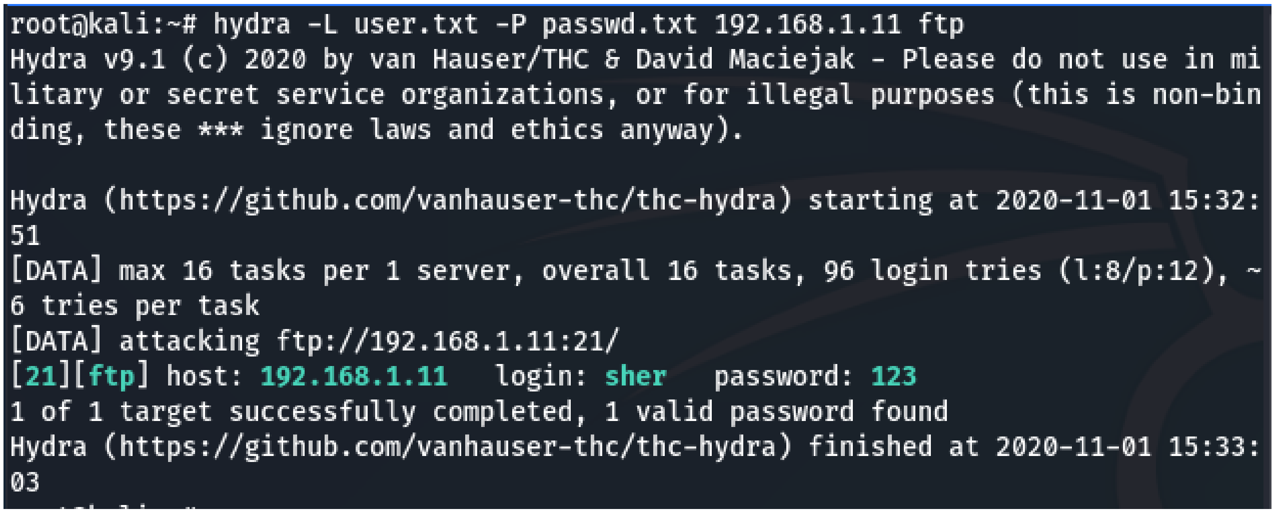


□	EVENT NAME	DATE GMT+5:30	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53814	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53814	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53814	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53814	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53814	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES Telnet password detected in cleartext"	2020-11-01 15:34:17	alienvault	N/A	Host-192-168-1-11:23	Host-192-168-1-12:53824	2->2	LOW (0)

Whoa ? as we can see it detected the multiple wrong login attempts.

Let's perform one more Brute Force attack Via FTP protocol to be ensured that it can detect all type of Brute Force attacks by simply running the following command:

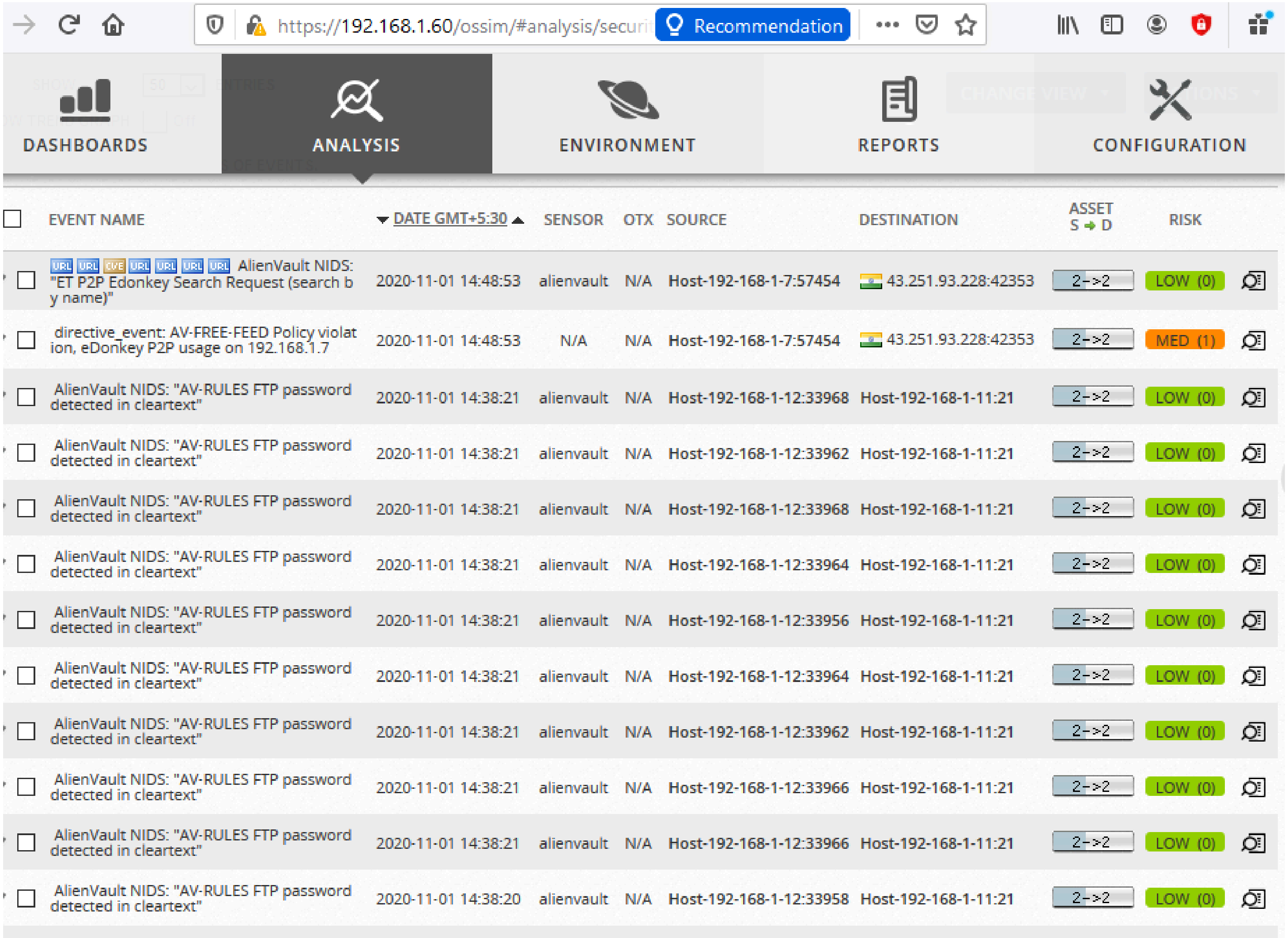
```
hydra -L user.txt -P passwd.txt 192.168.11 ftp
```



```
root@kali:~# hydra -L user.txt -P passwd.txt 192.168.1.11 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-01 15:32:
51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 96 login tries (l:8/p:12), ~
6 tries per task
[DATA] attacking ftp://192.168.1.11:21/
[21][ftp] host: 192.168.1.11   login: sher   password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-01 15:33:
03
```

Let's check the logs

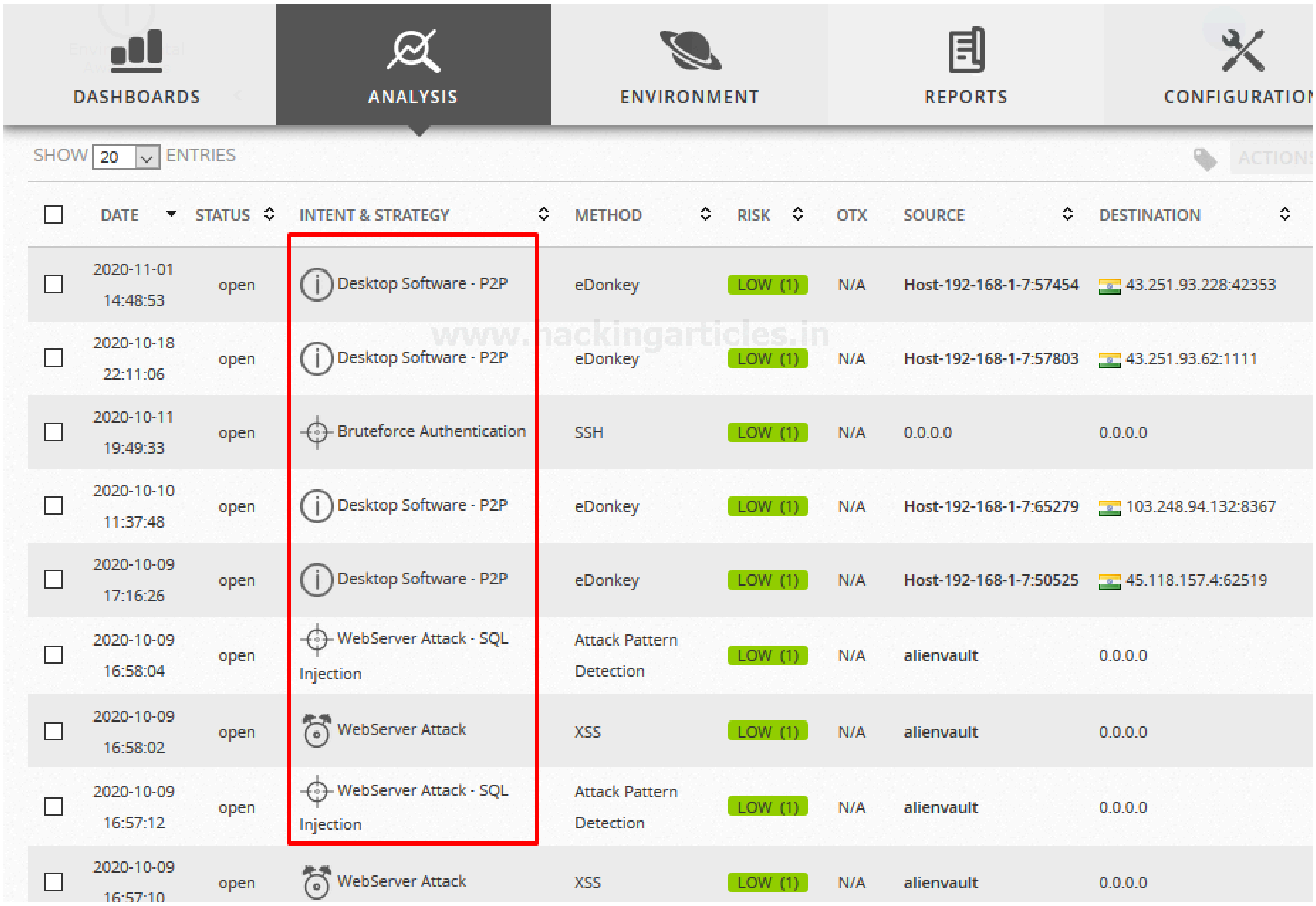


□	EVENT NAME	DATE GMT+5:30	SENSOR	OTX	SOURCE	DESTINATION	ASSET S ➜ D	RISK
□	URL URL CVE URL URL URL URL AlienVault NIDS: "ET P2P Edonkey Search Request (search by name)"	2020-11-01 14:48:53	alienvault	N/A	Host-192-168-1-7:57454	43.251.93.228:42353	2->2	LOW (0)
□	directive_event: AV-FREE-FEED Policy violation, eDonkey P2P usage on 192.168.1.7	2020-11-01 14:48:53	N/A	N/A	Host-192-168-1-7:57454	43.251.93.228:42353	2->2	MED (1)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33968	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33962	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33968	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33964	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33956	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33964	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33962	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33966	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:21	alienvault	N/A	Host-192-168-1-12:33966	Host-192-168-1-11:21	2->2	LOW (0)
□	AlienVault NIDS: "AV-RULES FTP password detected in cleartext"	2020-11-01 14:38:20	alienvault	N/A	Host-192-168-1-12:33958	Host-192-168-1-11:21	2->2	LOW (0)

As we can see it also detected multiple wrong logins attempts with the host or source details.

It’s quite informative to evade Brute force attacks.

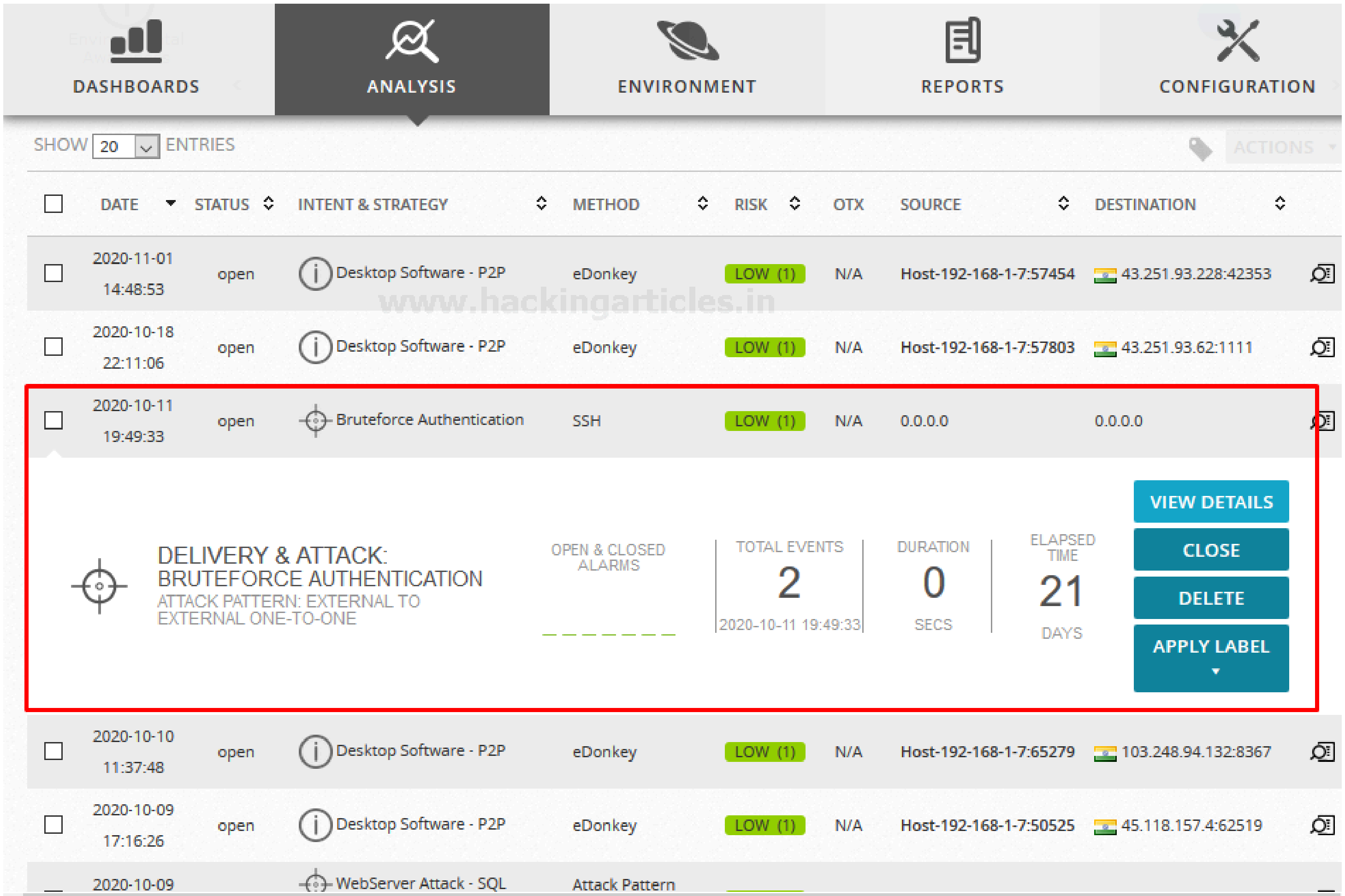
Similarly, I performed some attacks in my network and yessss…. AlienVault detected all the threats and generated Alarms smartly under Analysis > Alarms as shown below:



☐	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
☐	2020-11-01 14:48:53	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:57454	43.251.93.228:42353
☐	2020-10-18 22:11:06	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:57803	43.251.93.62:1111
☐	2020-10-11 19:49:33	open	Bruteforce Authentication	SSH	LOW (1)	N/A	0.0.0.0	0.0.0.0
☐	2020-10-10 11:37:48	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:65279	103.248.94.132:8367
☐	2020-10-09 17:16:26	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:50525	45.118.157.4:62519
☐	2020-10-09 16:58:04	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	alienvault	0.0.0.0
☐	2020-10-09 16:58:02	open	WebServer Attack	XSS	LOW (1)	N/A	alienvault	0.0.0.0
☐	2020-10-09 16:57:12	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	alienvault	0.0.0.0
☐	2020-10-09 16:57:10	open	WebServer Attack	XSS	LOW (1)	N/A	alienvault	0.0.0.0

Let’s check the host details from where or which type of attack were performed. As we can see the details of the Brute Force attack that above we have performed.

You can make it more informative by navigating to View Details.



SHOW 20 ENTRIES

□	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
□	2020-11-01 14:48:53	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:57454	43.251.93.228:42353
□	2020-10-18 22:11:06	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:57803	43.251.93.62:1111
□	2020-10-11 19:49:33	open	Bruteforce Authentication	SSH	LOW (1)	N/A	0.0.0.0	0.0.0.0
□	2020-10-10 11:37:48	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:65279	103.248.94.132:8367
□	2020-10-09 17:16:26	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-192-168-1-7:50525	45.118.157.4:62519
	2020-10-09		WebServer Attack - SQL	Attack Pattern				

DELIVERY & ATTACK: BRUTEFORCE AUTHENTICATION
ATTACK PATTERN: EXTERNAL TO EXTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS

TOTAL EVENTS 2
2020-10-11 19:49:33

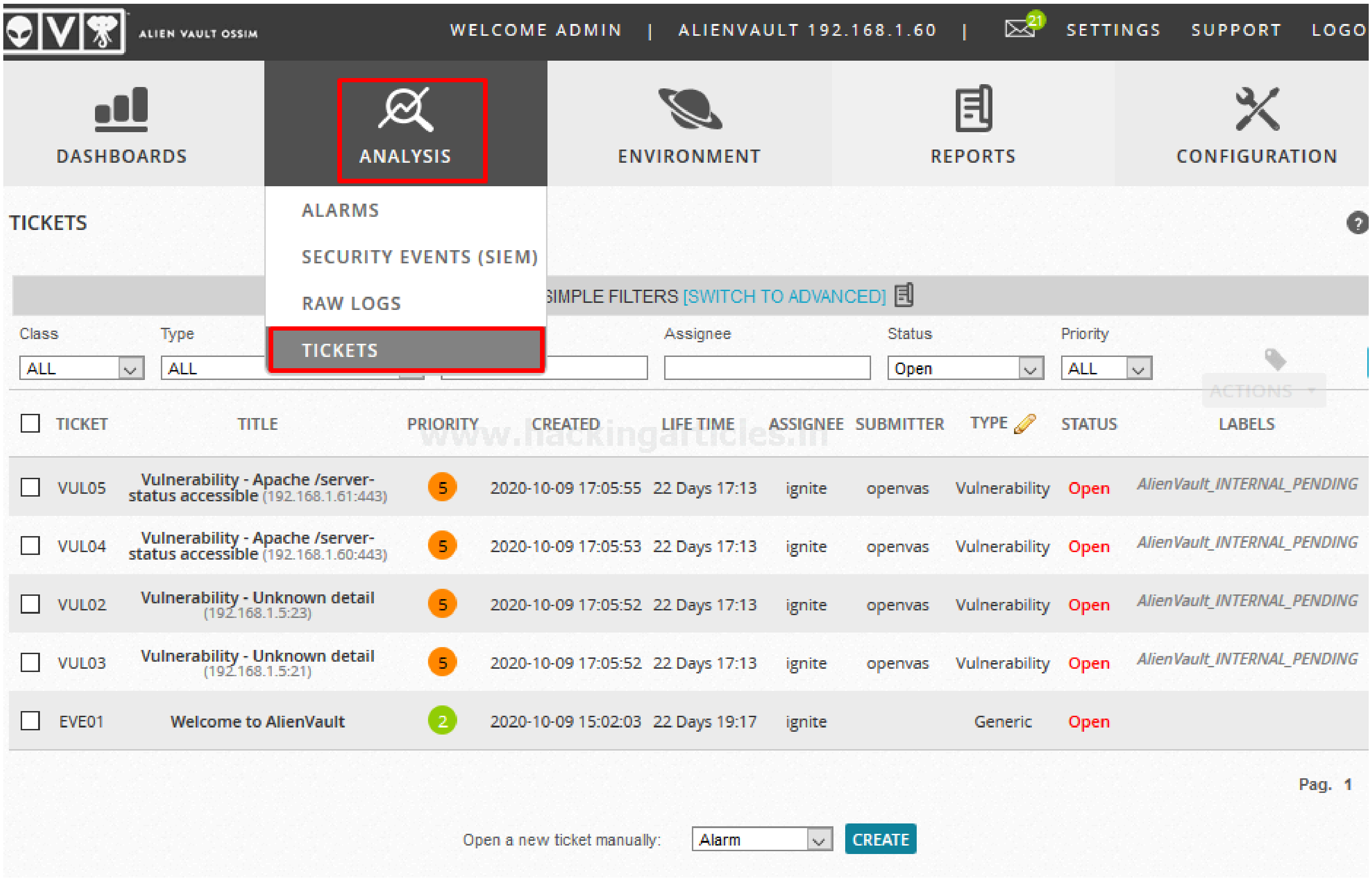
DURATION 0 SECS

ELAPSED TIME 21 DAYS

Alerts Attack based Tickets

It provides access to the OSSIM Appliance management system. Tickets are helpful to provide workflow tracking activity related to detected alarms such as vulnerabilities found in systems or applications or other issues that you want to keep track of.

Here OSSIM generated some tickets on behalf of performed automatic vulnerability scan or some on behalf of attack vector as shown below



TICKETS

Class: ALL | Type: ALL | Assignee: | Status: Open | Priority: ALL

□	TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	ASSIGNEE	SUBMITTER	TYPE	STATUS	LABELS
□	VUL05	Vulnerability - Apache /server-status accessible (192.168.1.61:443)	5	2020-10-09 17:05:55	22 Days 17:13	ignite	openvas	Vulnerability	Open	AlienVault_INTERNAL_PENDING
□	VUL04	Vulnerability - Apache /server-status accessible (192.168.1.60:443)	5	2020-10-09 17:05:53	22 Days 17:13	ignite	openvas	Vulnerability	Open	AlienVault_INTERNAL_PENDING
□	VUL02	Vulnerability - Unknown detail (192.168.1.5:23)	5	2020-10-09 17:05:52	22 Days 17:13	ignite	openvas	Vulnerability	Open	AlienVault_INTERNAL_PENDING
□	VUL03	Vulnerability - Unknown detail (192.168.1.5:21)	5	2020-10-09 17:05:52	22 Days 17:13	ignite	openvas	Vulnerability	Open	AlienVault_INTERNAL_PENDING
□	EVE01	Welcome to AlienVault	2	2020-10-09 15:02:03	22 Days 19:17	ignite		Generic	Open	

Pag. 1

Open a new ticket manually: Alarm

By default, the OSSIM appliance Web UI displays a list of all tickets. Also, you can click the Create button to create a new ticket of a specific type or category.

In the Filters section at the top of the Tickets page, you can choose criteria to filter the ticket results. You can choose additional criteria to filter ticket results by clicking the Switch to Advanced option.

From the Ticket summary list, you can click on a specific ticket to open the ticket and display the entire details of the ticket on a new page. From this ticket detail display, you can perform various actions such as editing fields in the ticket, assigning the ticket, adding notes and attachments, and changing the status and priority of a ticket, depending on whatever method or process you want to use to track resolution of issues.

Traffic Analysis

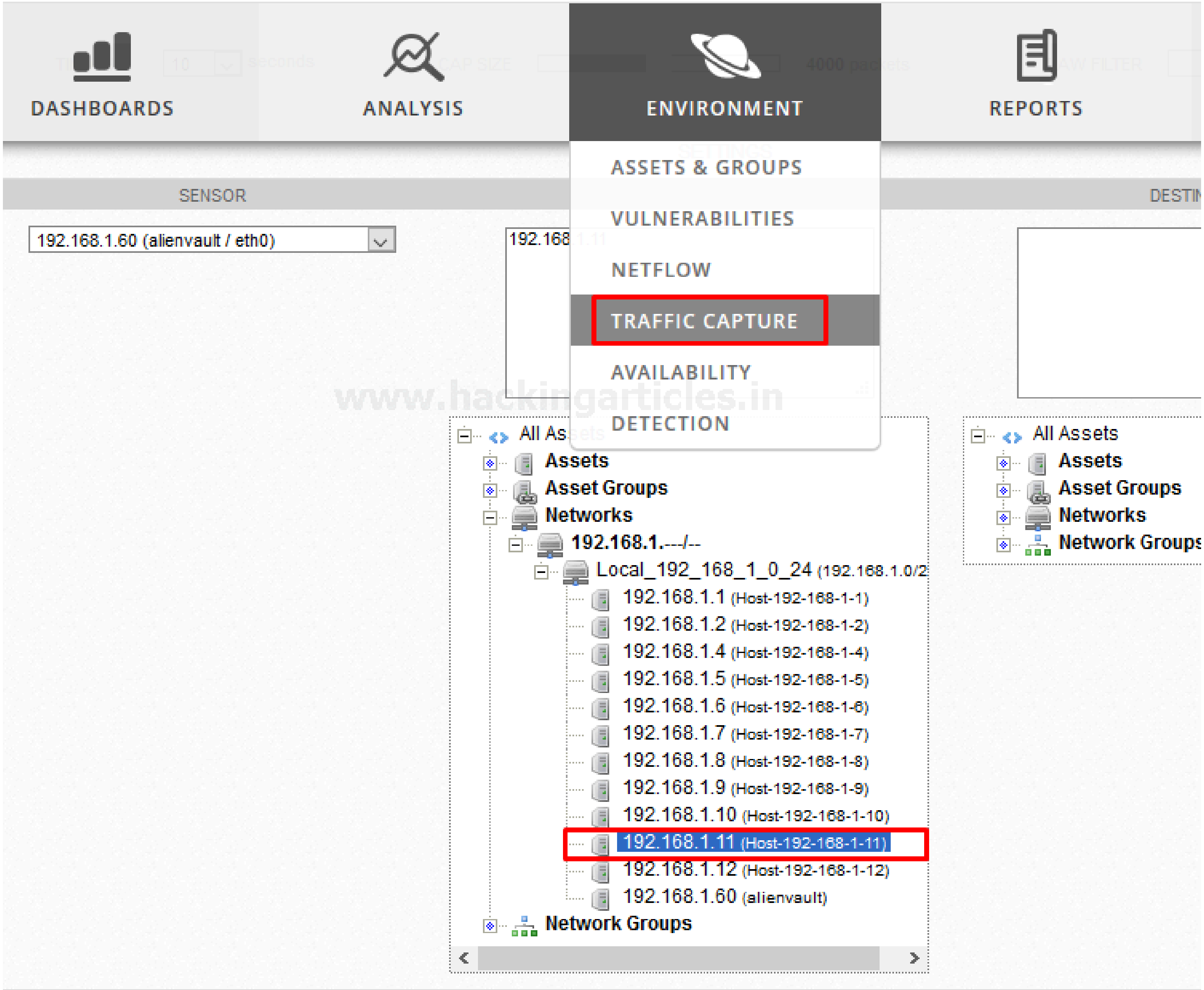
This option allows users to monitor or manage remote traffic capture through the OSSIM sensor.

There are few capture options available as shown below

- Timeout
- Filtering packet size
- Sensor name
- Packet source and destination

Let's check out how AlienVault perform Traffic Analysis

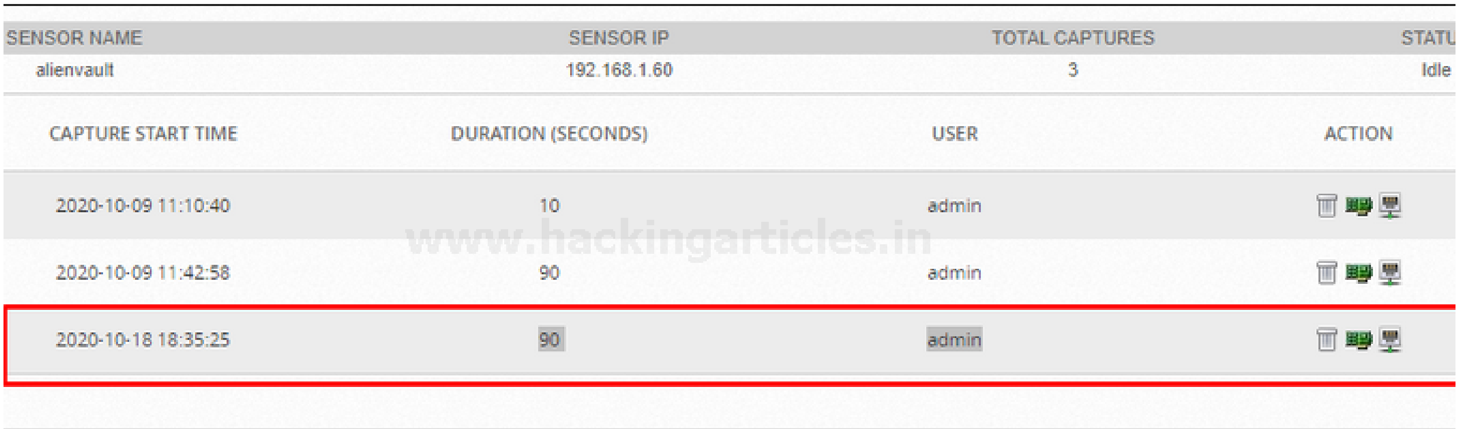
To perform Traffic Capture, navigate to **"Environment > Traffic Capture"** apply the filters as per your own in my case I choose timeout value 90 seconds and selected the source as shown below


DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
ASSETS & GROUPS
VULNERABILITIES
NETFLOW
TRAFFIC CAPTURE
AVAILABILITY
DETECTION
SENSOR
DESTI
All Assets
Assets
Asset Groups
Networks
192.168.1.---/--
Local_192_168_1_0_24 (192.168.1.0/2
192.168.1.1 (Host-192-168-1-1)
192.168.1.2 (Host-192-168-1-2)
192.168.1.4 (Host-192-168-1-4)
192.168.1.5 (Host-192-168-1-5)
192.168.1.6 (Host-192-168-1-6)
192.168.1.7 (Host-192-168-1-7)
192.168.1.8 (Host-192-168-1-8)
192.168.1.9 (Host-192-168-1-9)
192.168.1.10 (Host-192-168-1-10)
192.168.1.11 (Host-192-168-1-11)
192.168.1.12 (Host-192-168-1-12)
192.168.1.60 (alienvault)
Network Groups
All Assets
Assets
Asset Groups
Networks
Network Groups
www.hackingarticles.in

SENSOR: 192.168.1.60 (alienvault / eth0)

192.168.1.11

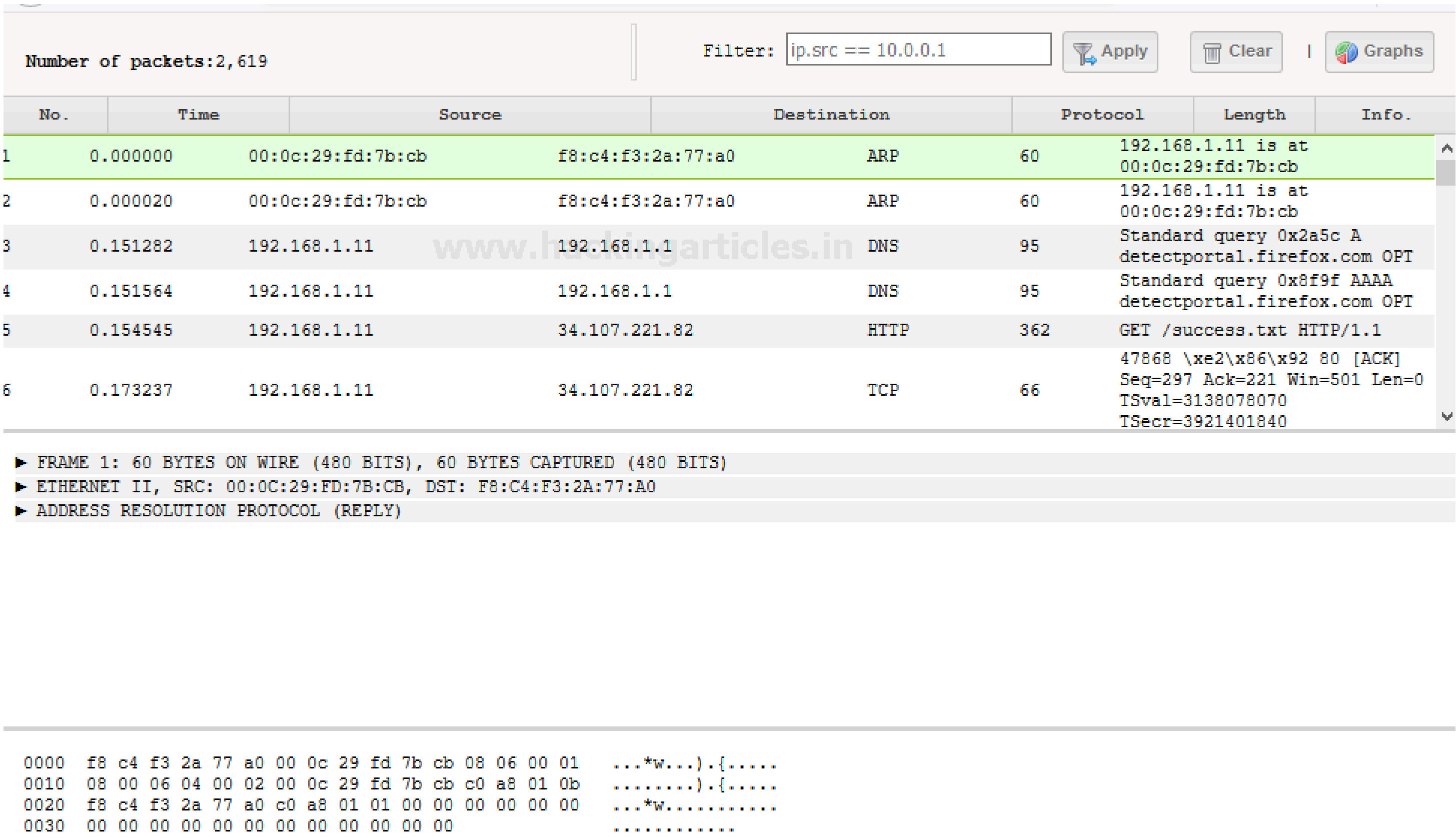
After Launching the traffic capture it saves the results in the upper section as shown below



SENSOR NAME	SENSOR IP	TOTAL CAPTURES	STATU
alienvault	192.168.1.60	3	Idle

CAPTURE START TIME	DURATION (SECONDS)	USER	ACTION
2020-10-09 11:10:40	10	admin	
2020-10-09 11:42:58	90	admin	
2020-10-18 18:35:25	90	admin	

As you can see it save the report in **PCAP** format you can see it directly by selecting the interface icon



Number of packets:2,619

Filter: ip.src == 10.0.0.1

No.	Time	Source	Destination	Protocol	Length	Info.
1	0.000000	00:0c:29:fd:7b:cb	f8:c4:f3:2a:77:a0	ARP	60	192.168.1.11 is at 00:0c:29:fd:7b:cb
2	0.000020	00:0c:29:fd:7b:cb	f8:c4:f3:2a:77:a0	ARP	60	192.168.1.11 is at 00:0c:29:fd:7b:cb
3	0.151282	192.168.1.11	192.168.1.1	DNS	95	Standard query 0x2a5c A detectportal.firefox.com OPT
4	0.151564	192.168.1.11	192.168.1.1	DNS	95	Standard query 0x8f9f AAAA detectportal.firefox.com OPT
5	0.154545	192.168.1.11	34.107.221.82	HTTP	362	GET /success.txt HTTP/1.1
6	0.173237	192.168.1.11	34.107.221.82	TCP	66	47868 \xe2\x86\x92 80 [ACK] Seq=297 Ack=221 Win=501 Len=0 TSval=3138078070 TSecr=3921401840

```
▶ FRAME 1: 60 BYTES ON WIRE (480 BITS), 60 BYTES CAPTURED (480 BITS)
▶ ETHERNET II, SRC: 00:0C:29:FD:7B:CB, DST: F8:C4:F3:2A:77:A0
▶ ADDRESS RESOLUTION PROTOCOL (REPLY)
```

```
0000  f8 c4 f3 2a 77 a0 00 0c 29 fd 7b cb 08 06 00 01   ...*w...).{.....
0010  08 00 06 04 00 02 00 0c 29 fd 7b cb c0 a8 01 0b   ........).{.....
0020  f8 c4 f3 2a 77 a0 c0 a8 01 01 00 00 00 00 00 00   ...*w...........
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

As we can see it capture different type of packets such as UDP or TCP.

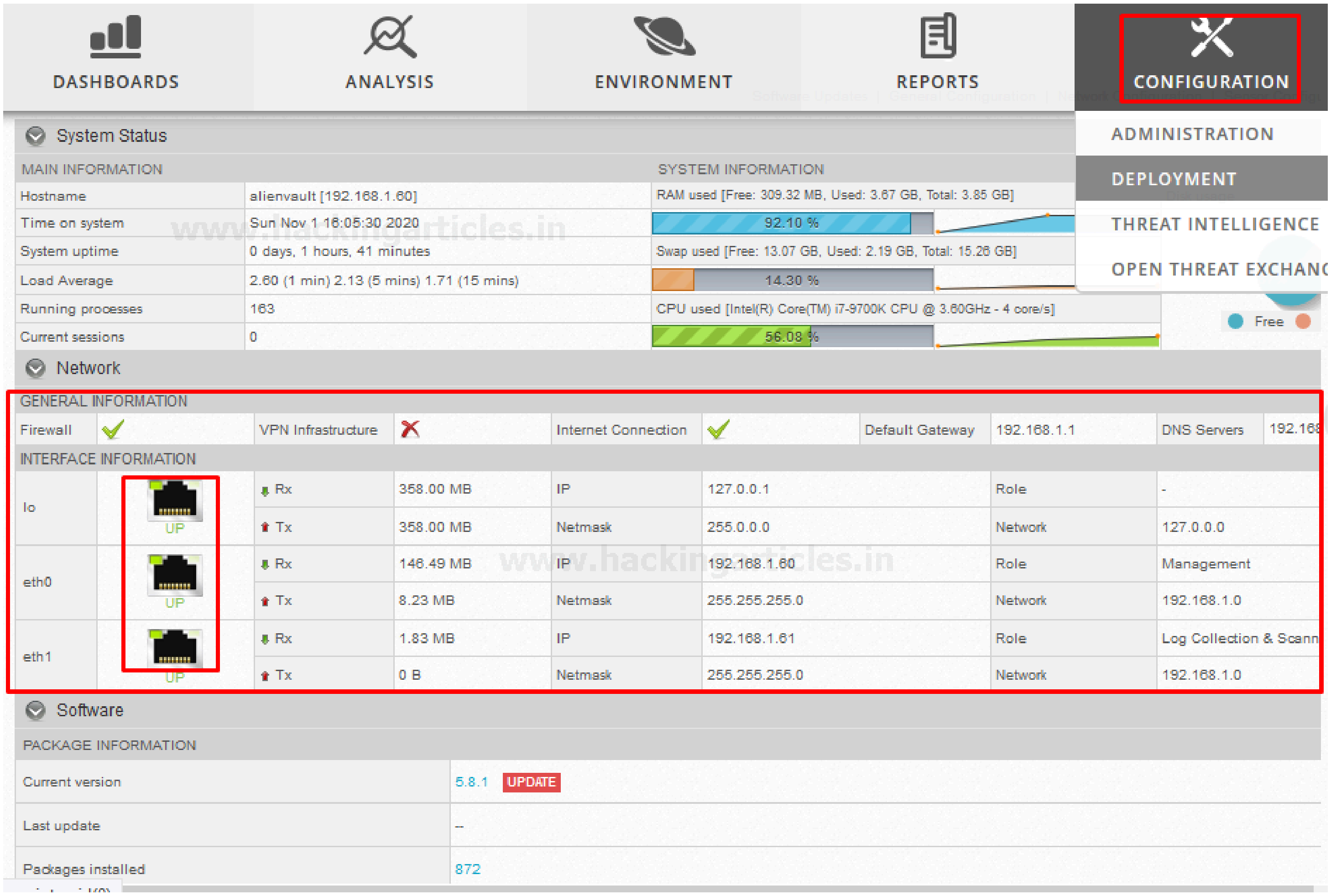
Similarly, you can monitor your whole network.

Deployment status

The default “**Configuration > Deployment**” provides status and resource information for different OSSIM Appliance instance components also it provides options to configure and manage OSSIM Appliance components such as:

- AlienVault sensors
- OSSIM appliance servers
- OSSIM Appliance loggers

So that you can view and change configuration settings for existing components as shown below:



System Status

MAIN INFORMATION		SYSTEM INFORMATION
Hostname	alienvault [192.168.1.60]	RAM used [Free: 309.32 MB, Used: 3.67 GB, Total: 3.85 GB]
Time on system	Sun Nov 1 16:05:30 2020	92.10 %
System uptime	0 days, 1 hours, 41 minutes	Swap used [Free: 13.07 GB, Used: 2.19 GB, Total: 15.26 GB]
Load Average	2.60 (1 min) 2.13 (5 mins) 1.71 (15 mins)	14.30 %
Running processes	163	CPU used [Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz - 4 core/s]
Current sessions	0	56.08 %

Network

GENERAL INFORMATION

Firewall	✓	VPN Infrastructure	✗	Internet Connection	✓	Default Gateway	192.168.1.1	DNS Servers	192.168

INTERFACE INFORMATION

lo	UP	Rx	358.00 MB	IP	127.0.0.1	Role	-
		Tx	358.00 MB	Netmask	255.0.0.0	Network	127.0.0.0
eth0	UP	Rx	146.49 MB	IP	192.168.1.60	Role	Management
		Tx	8.23 MB	Netmask	255.255.255.0	Network	192.168.1.0
eth1	UP	Rx	1.83 MB	IP	192.168.1.61	Role	Log Collection & Scann
		Tx	0 B	Netmask	255.255.255.0	Network	192.168.1.0

Software

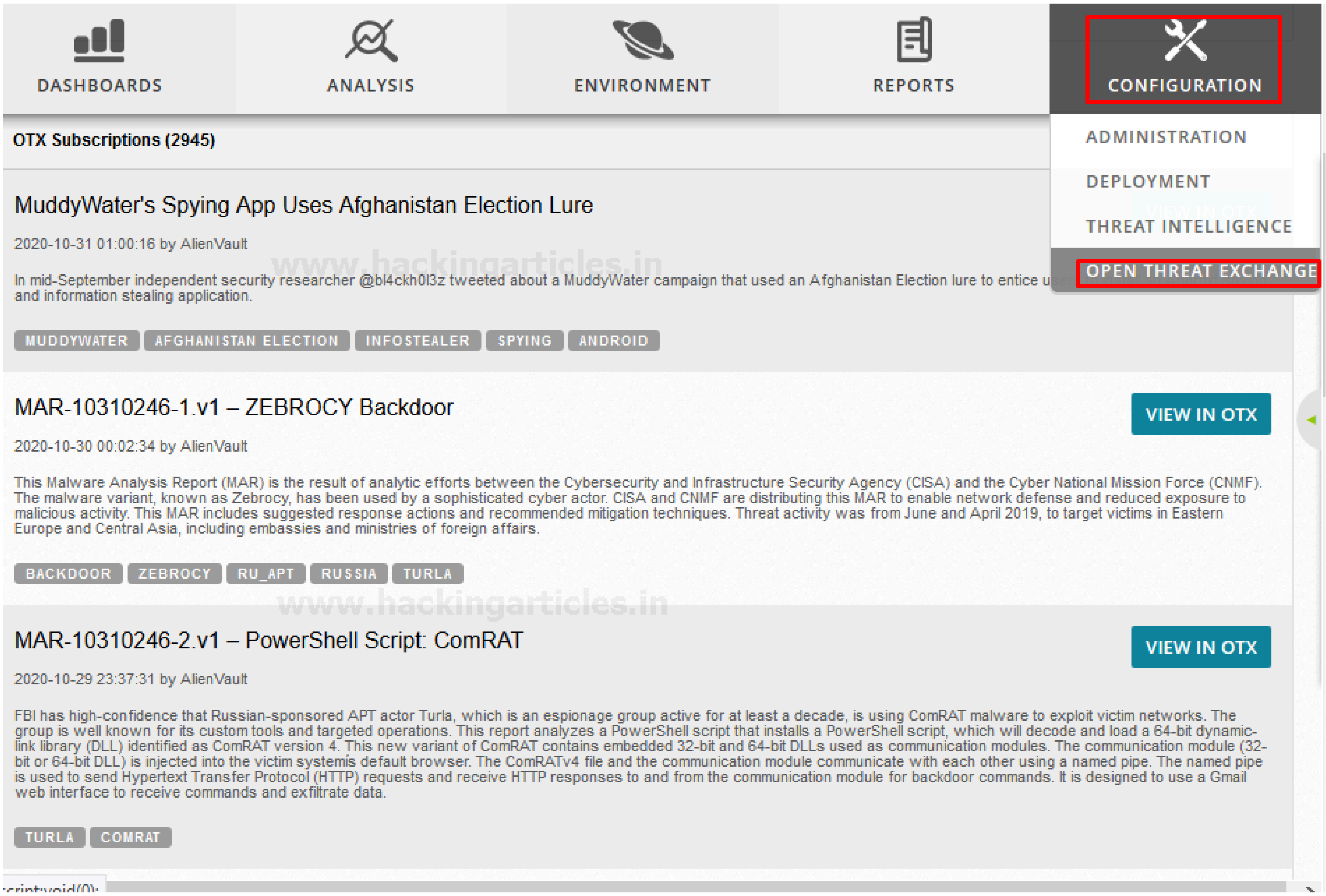
PACKAGE INFORMATION

Current version	5.8.1 UPDATE
Last update	--
Packages installed	872

OTX: Open Threat Exchange

OTX is an open information-sharing and analysis network that provides access to real-time information about issues and attack threats that may impact your organization, allowing you to learn from and work with others who have already experienced such attacks. AT&T Alien Labs™ and other security researchers constantly monitor, analyze, reverse engineer, and report on sophisticated threats including malware, botnets, phishing campaigns, and more.

Navigate to "**Configuration > Open Threat Exchange option**", OSSIM Appliance displays the following page.



OTX Subscriptions (2945)

MuddyWater's Spying App Uses Afghanistan Election Lure

2020-10-31 01:00:16 by AlienVault

In mid-September independent security researcher @bl4ckh0l3z tweeted about a MuddyWater campaign that used an Afghanistan Election lure to entice u
and information stealing application.

MAR-10310246-1.v1 – ZEBROCY Backdoor

2020-10-30 00:02:34 by AlienVault

This Malware Analysis Report (MAR) is the result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber National Mission Force (CNMF). The malware variant, known as Zebrocy, has been used by a sophisticated cyber actor. CISA and CNMF are distributing this MAR to enable network defense and reduced exposure to malicious activity. This MAR includes suggested response actions and recommended mitigation techniques. Threat activity was from June and April 2019, to target victims in Eastern Europe and Central Asia, including embassies and ministries of foreign affairs.

MAR-10310246-2.v1 – PowerShell Script: ComRAT

2020-10-29 23:37:31 by AlienVault

FBI has high-confidence that Russian-sponsored APT actor Turla, which is an espionage group active for at least a decade, is using ComRAT malware to exploit victim networks. The group is well known for its custom tools and targeted operations. This report analyzes a PowerShell script that installs a PowerShell script, which will decode and load a 64-bit dynamic-link library (DLL) identified as ComRAT version 4. This new variant of ComRAT contains embedded 32-bit and 64-bit DLLs used as communication modules. The communication module (32-bit or 64-bit DLL) is injected into the victim systemís default browser. The ComRATv4 file and the communication module communicate with each other using a named pipe. The named pipe is used to send Hypertext Transfer Protocol (HTTP) requests and receive HTTP responses to and from the communication module for backdoor commands. It is designed to use a Gmail web interface to receive commands and exfiltrate data.

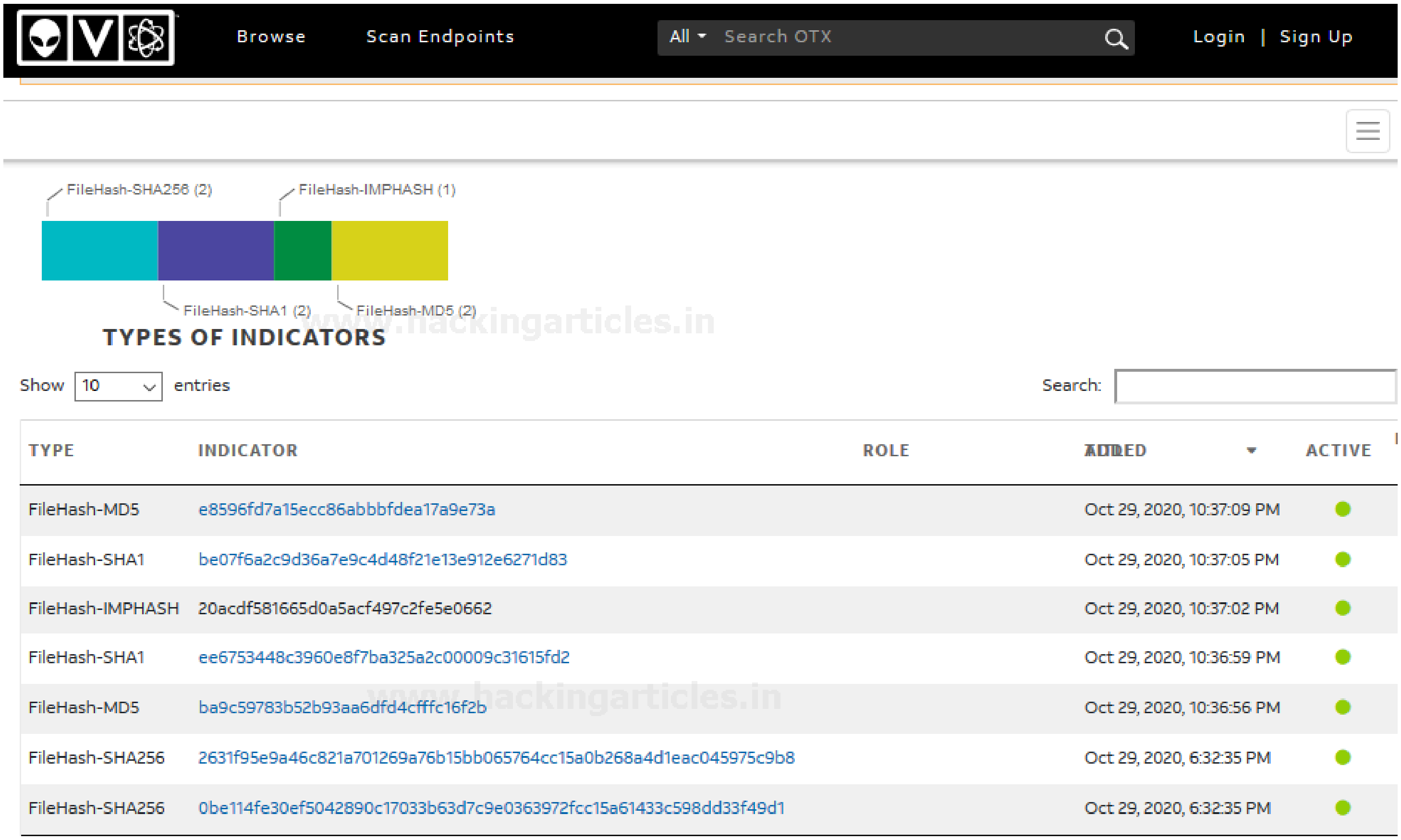
Indicators of compromise (IoCs)

Threat hunting generally begins with security analysts working through threat intelligence, understanding of the environment they secure, and other security data sources to postulate about a potential threat. Threat hunters then look for indicators of compromise (IoCs) found in forensic “artifacts” to identify threatening activity that aligns with the hypothesized threat activity.

These artifacts are bits of data from server logs, network traffic, configurations, and more that help threat hunters determine if suspicious activities have taken place. Artifacts include:

- Network-based artifacts – Monitoring listening ports of internet-facing systems, threat hunters can monitor traffic as well as look through packet session recordings, looking for unusual outbound traffic, abnormal communication geographies, irregular amounts of inbound or outbound data, etc.
- Host-based artifacts – Changes in file systems and the Windows registry are two places threat hunters can find anomalous settings and content. Scanning registry values and monitoring changes made to file systems are common threat hunting activities.
- Authentication-based artifacts – Monitoring or reviewing the login (or attempted login) of privileged accounts on endpoints, servers, and services can be useful for a threat hunter to follow the trail used by an attacker to identify which accounts have been compromised and need to be remediated.

You can perform Threat hunting on behalf of OTX IoCs by opening them “**View in OTX”** as shown below:



TYPES OF INDICATORS

Show 10 entries

Search:

TYPE	INDICATOR	ROLE	ADDED	ACTIVE
FileHash-MD5	e8596fd7a15ecc86abbbfdea17a9e73a		Oct 29, 2020, 10:37:09 PM	●
FileHash-SHA1	be07f6a2c9d36a7e9c4d48f21e13e912e6271d83		Oct 29, 2020, 10:37:05 PM	●
FileHash-IMPHASH	20acdf581665d0a5acf497c2fe5e0662		Oct 29, 2020, 10:37:02 PM	●
FileHash-SHA1	ee6753448c3960e8f7ba325a2c00009c31615fd2		Oct 29, 2020, 10:36:59 PM	●
FileHash-MD5	ba9c59783b52b93aa6dfd4cfffc16f2b		Oct 29, 2020, 10:36:56 PM	●
FileHash-SHA256	2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8		Oct 29, 2020, 6:32:35 PM	●
FileHash-SHA256	0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1		Oct 29, 2020, 6:32:35 PM	●

The path taken during the “hunt” is only defined by the details discovered. For example, spotting anomalous outbound network traffic would lead a threat hunter to take a closer look at the endpoint transmitting that traffic. Thus, there’s no one established threat hunting process that applies to every hunt.

Let’s end up here.

Reference: – Source: – **AlienVault AT&T Cybersecurity**