CySA+ Lab Series

Lab 20: Network Intrusion Detection with OSSIM

Document Version: 2022-10-10

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.3 - Given a scenario, perform vulnerability management activities 1.4 - Given a scenario, analyze the output from common vulnerability tools 1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities 3.1 - Given a scenario, analyze data as part of security monitoring activities 3.2 - Given a scenario, implement configuration changes to existing controls to improve security 3.4 - Compare and Contrast automation concepts and technologies 4.2 - Given a scenario, apply the appropriate incident response procedure 4.3 - Given an incident, analyze potential indicators of compromise 5.2 - Given a scenario, apply security concepts in support of organizational risk mitigation
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	3: Vulnerability Management Activities 4: Vulnerability Assessment Tools 7: Mitigating Controls for Attacks and Software Vulnerabilities 11: Data Analysis in Security Monitoring Activities 12: Implement Configuration Changes to Existing Controls to Improve Security 14: Automation Concepts and Technologies 16: Appropriate Incident Response Procedures 17: Analyze Potential Indicators of Compromise 20: Security Concepts in Support of Organizational Risk Mitigation

Contents

Introduction

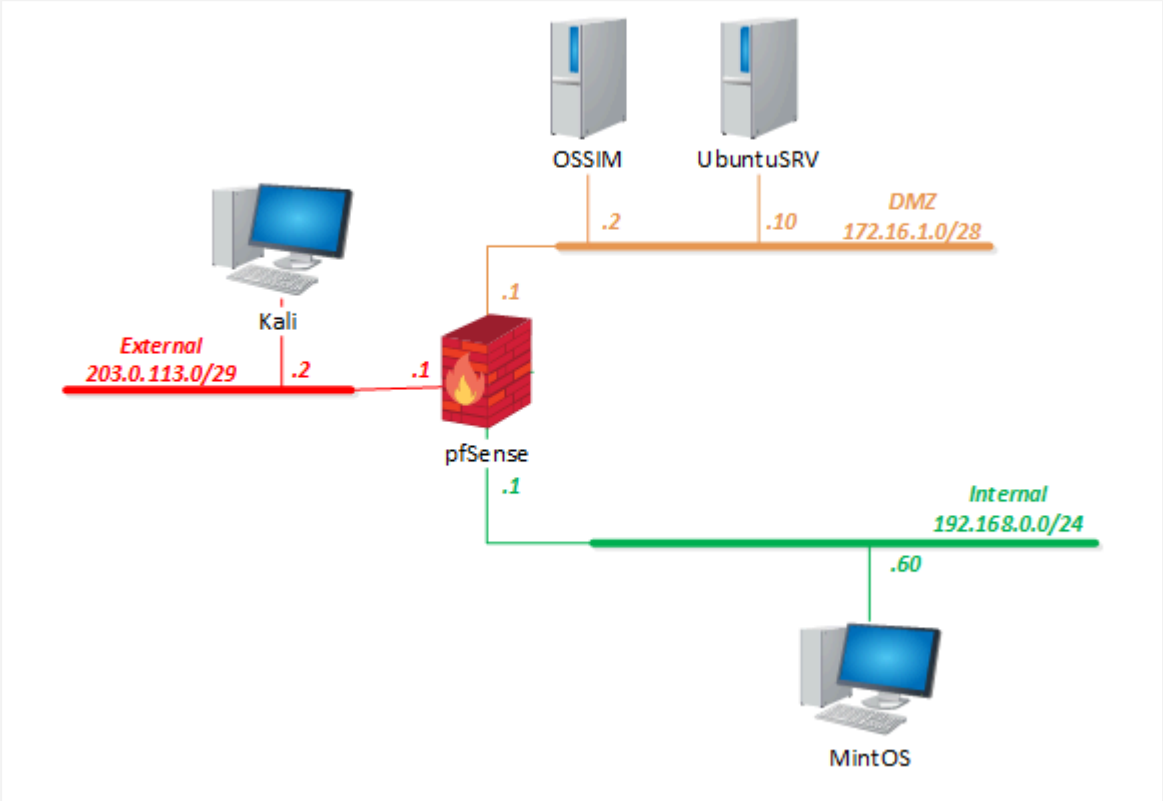
In *Lab 19: Creating New Rules and Testing IDS/IPS Using Snort,* you looked at *Snort*, an addition to a firewall that provides an intrusion detection application with a rich set of rules, logs packets for detailed analysis, and many other features. While *Snort* has a lightweight footprint and is easily integrated into the *pfSense* firewall, and is good at providing IDS/IPS functionality, it is not a Unified Security Management appliance, which is more adept at detecting advanced threats. *AlienVault OSSIM* includes powerful IDS/IPS functionality as well as asset discovery, vulnerability assessment, behavioral monitoring, and Security Information and Event Management (SIEM).

In this lab, you will be reviewing intrusion detection techniques for the *AlienVault OSSIM* system by generating *NIDS* events, creating custom status views, reviewing alarms, and creating reports.

Objectives

- Generating NIDS Events
- Create Custom Status Views
- Review Alarms (using *Suricata* Rules)
- Creating Reports

Lab Topology



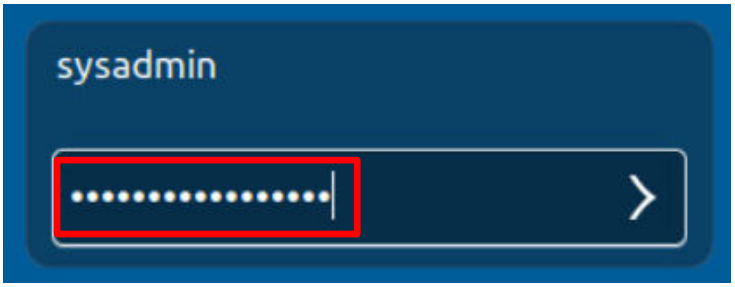
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

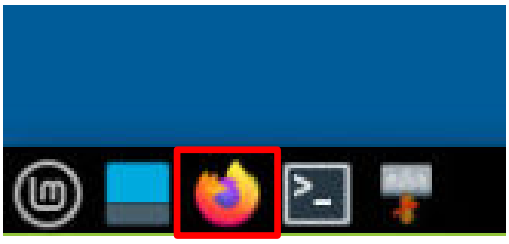
Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	192.168.0.50	Administrator	NDGlabpass123!
MintOS (Linux Mint)	192.168.0.60	sysadmin	NDGlabpass123!
OSSIM (AlienVault)	172.16.1.2	root	NDGlabpass123!
UbuntuSRV (Ubuntu Server)	172.16.1.10	sysadmin	NDGlabpass123!
Kali	203.0.113.2	sysadmin	NDGlabpass123!
pfSense	203.0.113.1 172.16.1.1 192.168.0.1	admin	NDGlabpass123!

1 Accessing AlienVault OSSIM

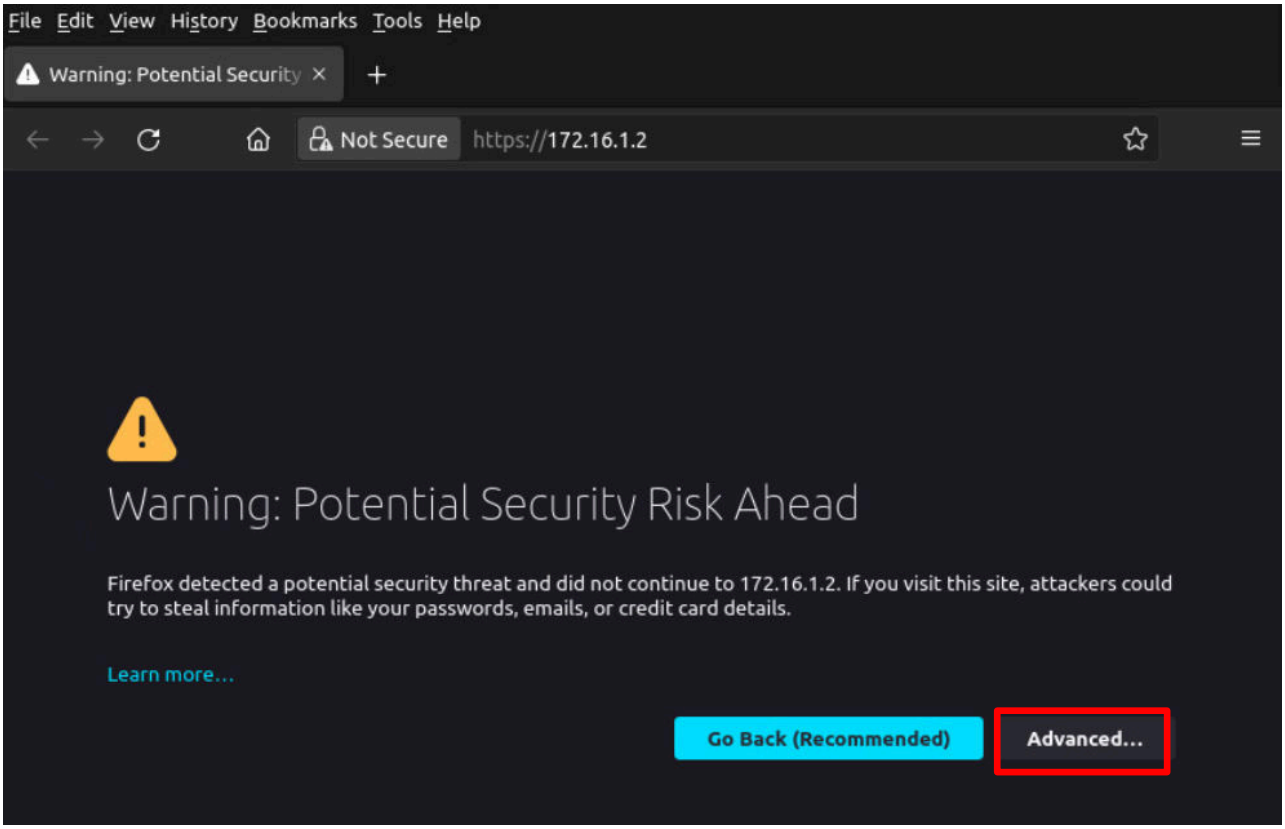
1. Set the focus on the **MintOS** computer.
2. Log in to the *sysadmin* account using the password: `NDGlabpass123!`



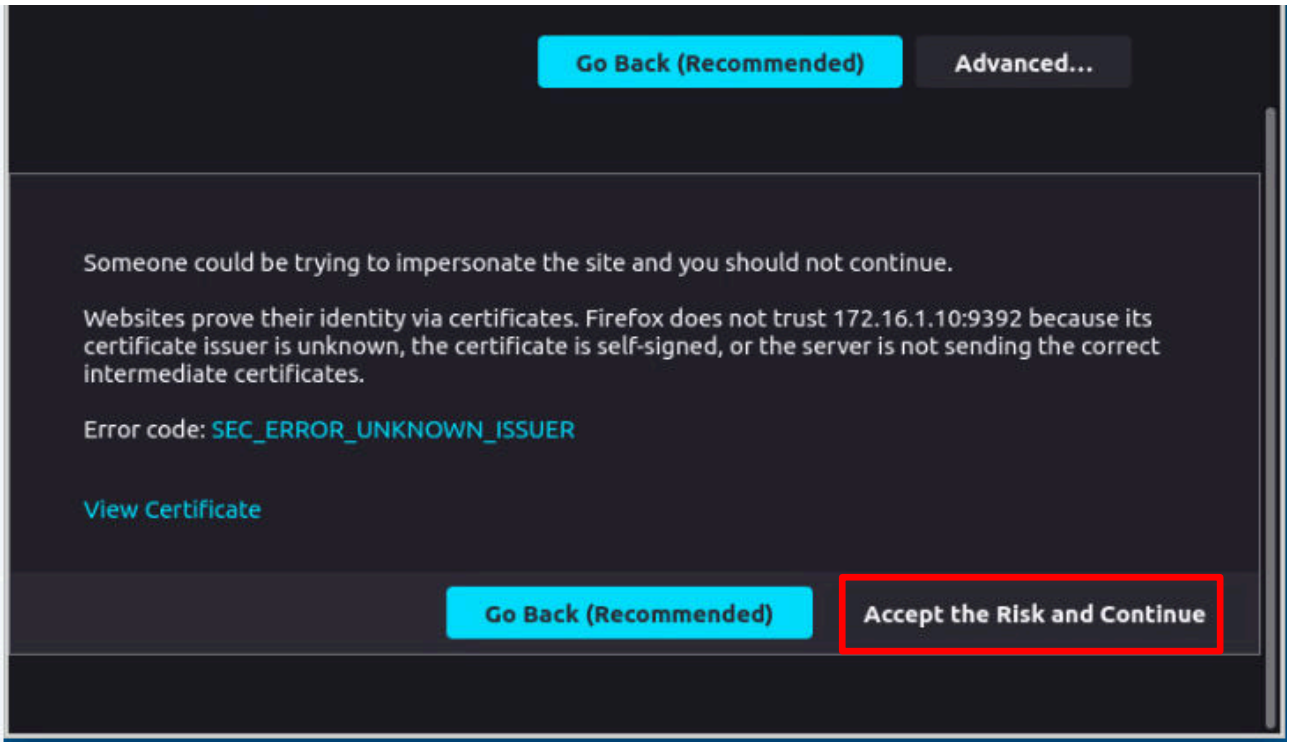
3. Open the browser by clicking on the **Firefox** icon located in the toolbar at the bottom of the window.



4. In the address bar of the browser, type the IP address of the OSSIM appliance, `172.16.1.2`.
5. On the *Warning: Potential Security Risk Ahead*, click on the **Advanced** button.

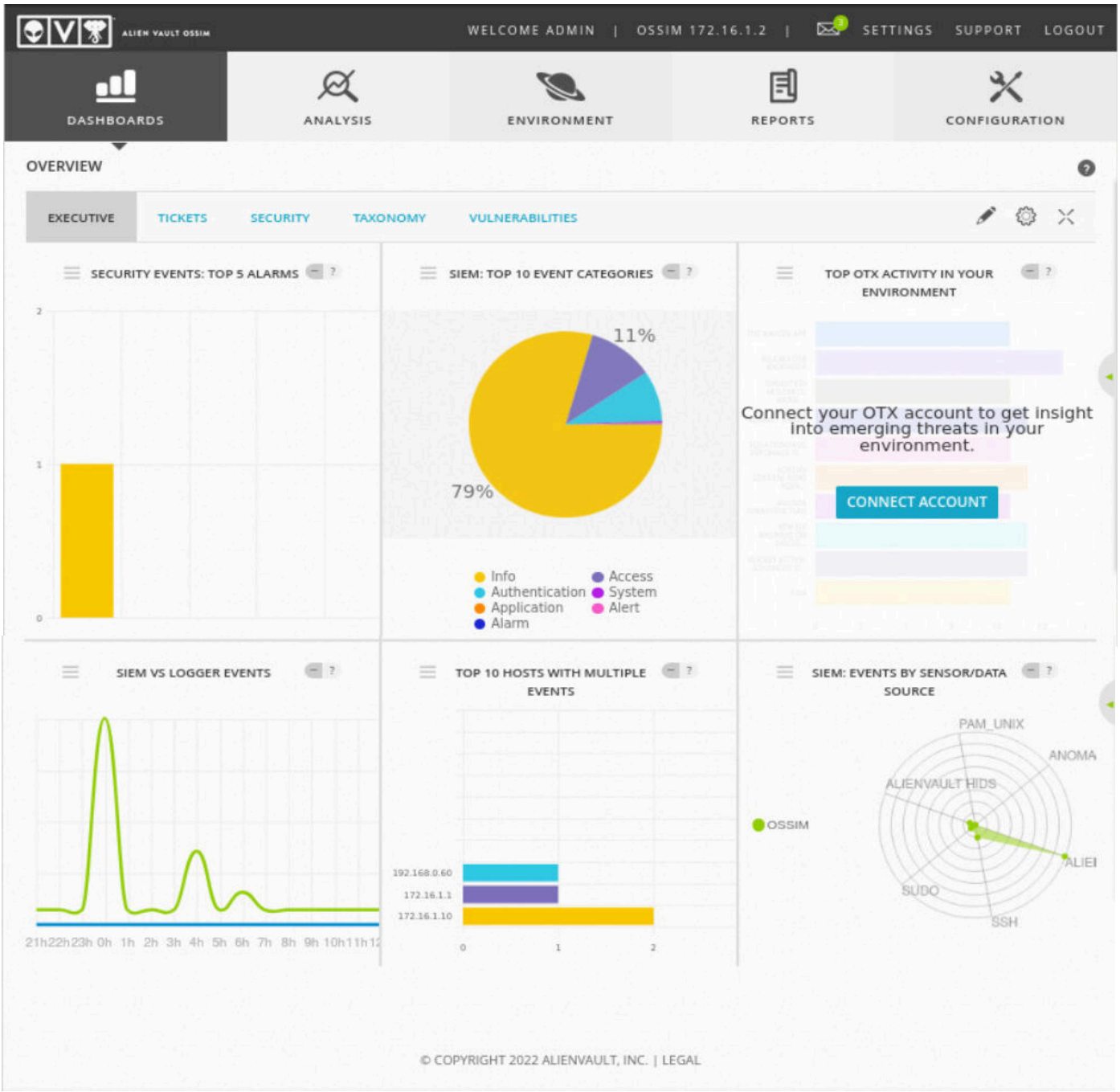


6. Scroll to the bottom of the window and click the **Accept the Risk and Continue** button.



7. Log in as `admin` using the password `NDGlabpass123!` and click the **LOGIN** button.

8. You will see the *AlienVault OSSIM Dashboard*. It displays a collection of graphs and charts that provides a high-level overview of network activity as it relates to security events and issues.



The primary menu on the top of the page shows the main operations of *OSSIM*, including:

Dashboards	Displays a broad overview of the OSSIM appliance, including security events, OTX activity, and network activity.
Analysis	Provides selections for filtering, searching, sorting, and selecting alarms, security events (SIEM), raw logs, and tickets.
Environment	Provides selections for the display and management of Assets and Groups, Vulnerabilities, Netflow data, Traffic Capture, Availability, and Detection.
Reports	Provides selections for the display and management of built-in reports based on categories such as alarms, assets, compliance, raw logs, security operations, and tickets. Custom reports can also be created and generated.
Configuration	Provides options for managing the OSSIM Appliance. Managing includes administrative, user, system configuration, and maintenance.

2 NIDS Event Monitoring and Reporting

A Network-Based Intrusion Detection System (*NIDS*) is a part of a Unified Security Management (*USM*) system that monitors and analyzes network traffic to protect the enterprise from network-based threats. *AlienVault OSSIM* comes with *NIDS* enabled.

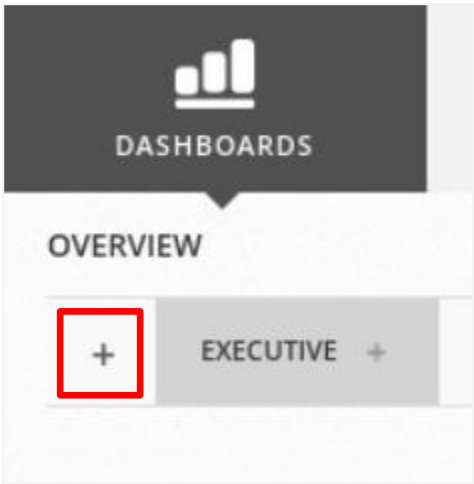
In this task, you will generate network traffic that will alert *NIDS* that a potential network threat has been detected and then send an alert for identification and analysis.

2.1 Create a Custom Dashboard View Showing NIDS Events

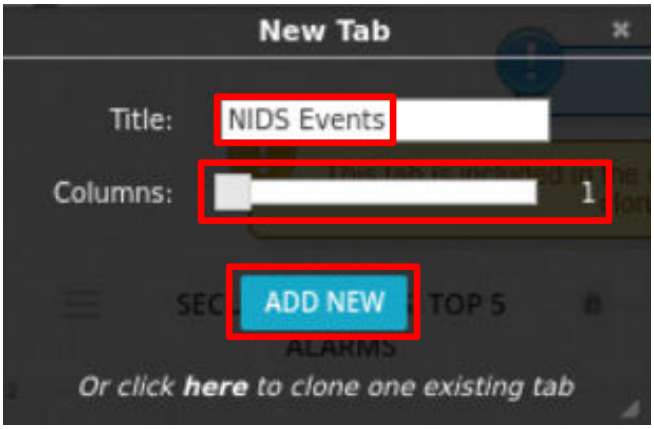
1. On the top-level menu, hover over **DASHBOARDS** and click **Overview**.

On the right side of the page, click on the **Switch to Edit Mode** icon (the pencil).

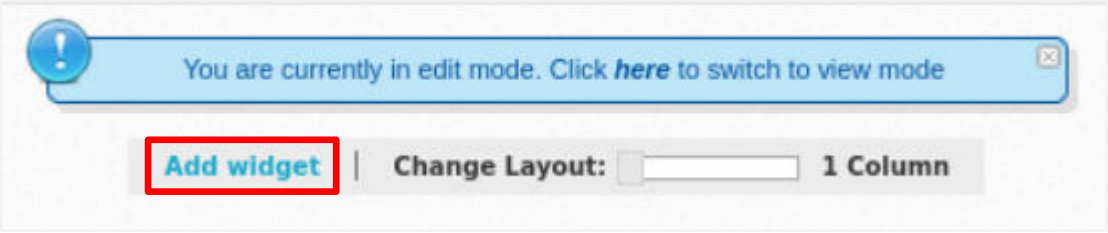
2. You will be in the **Edit Mode** for the *Dashboard*. Click on the **+** icon on the left side of the *Tab* list.



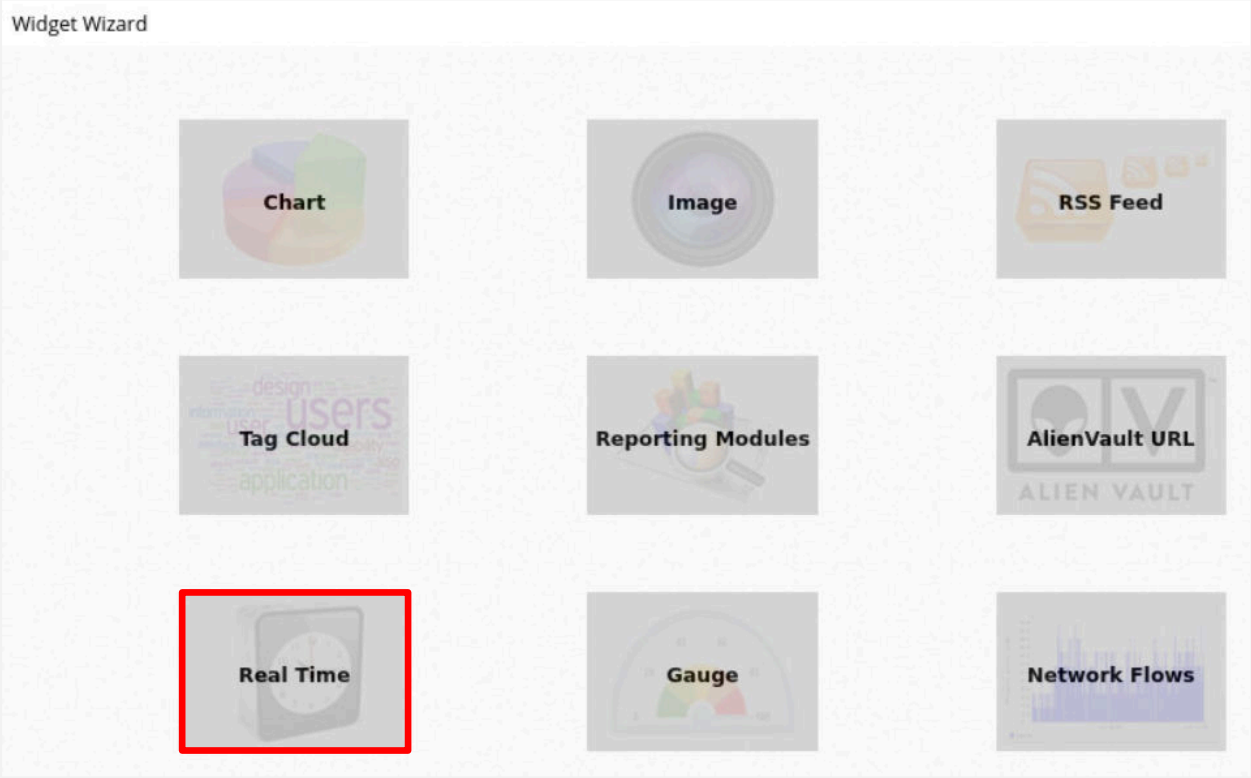
3. In the *New Tab* window, type `NIDS Events` for the *Title* and move the slider to **1** in *Columns*. Then click on **ADD NEW** button.



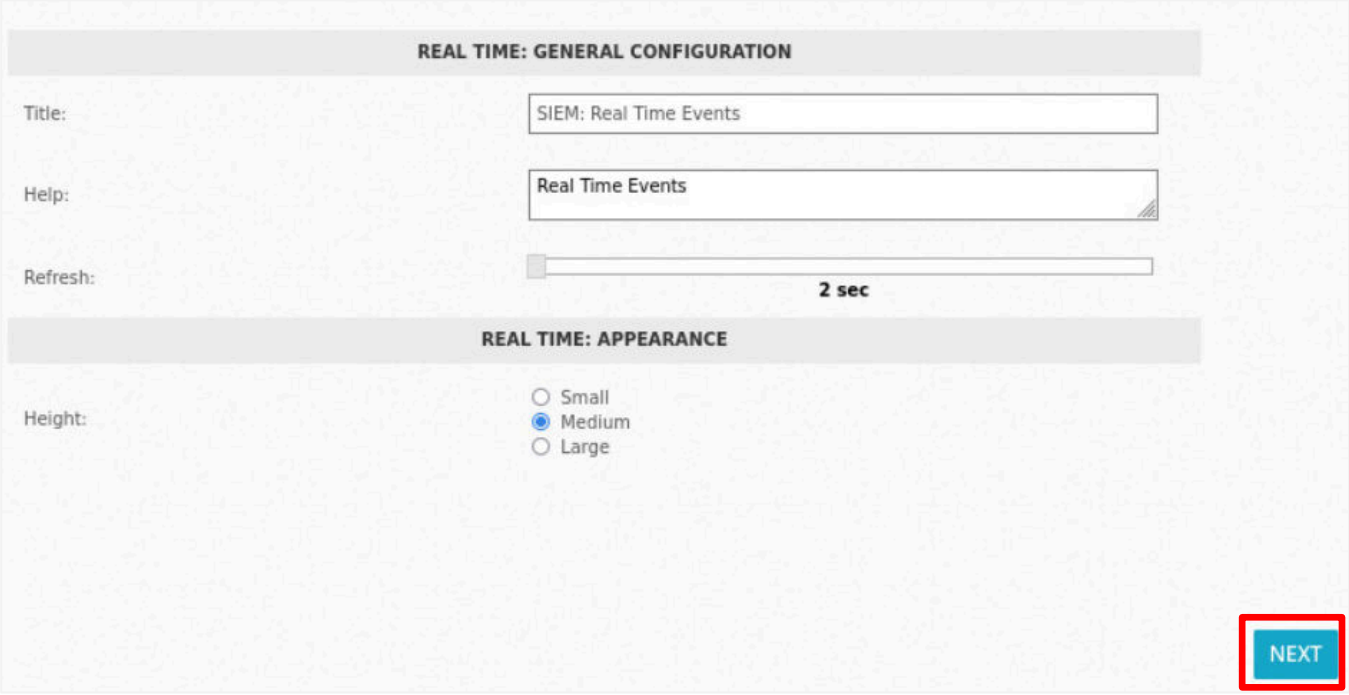
4. Click on the **Add Widget** link.



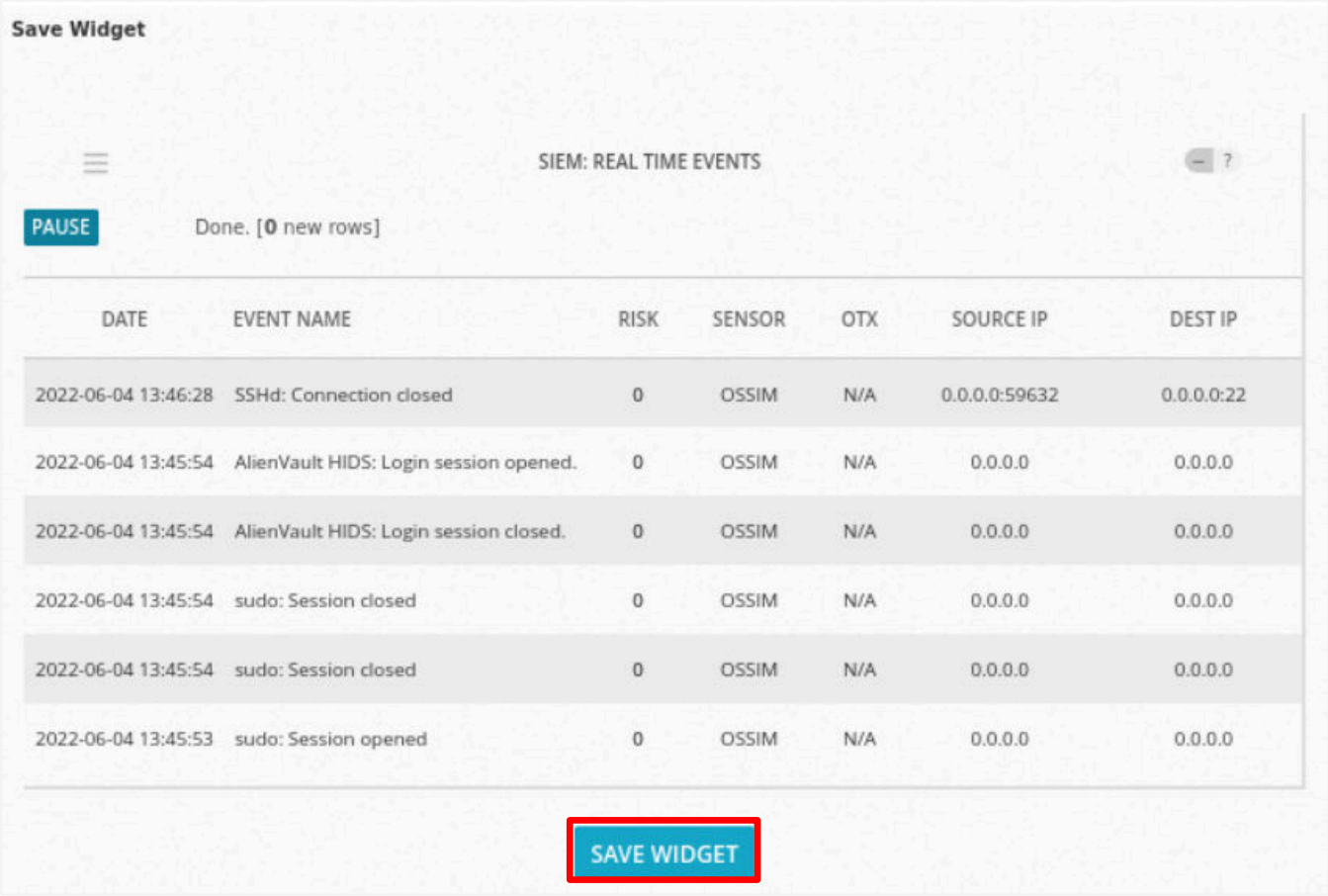
5. On the *Widget Wizard* page, click on **Real Time.**



6. On the *Customize Widget* page, leave the default settings for both *REAL TIME: GENERAL CONFIGURATION* and *REAL TIME: APPEARANCE* and click **NEXT.**

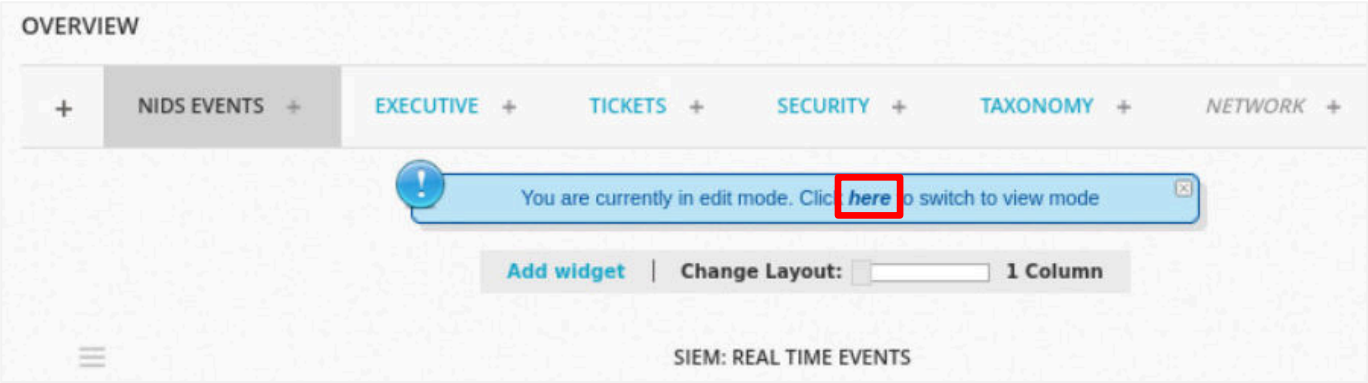


7. On the *Save Widget* page, click on the **SAVE WIDGET** button.

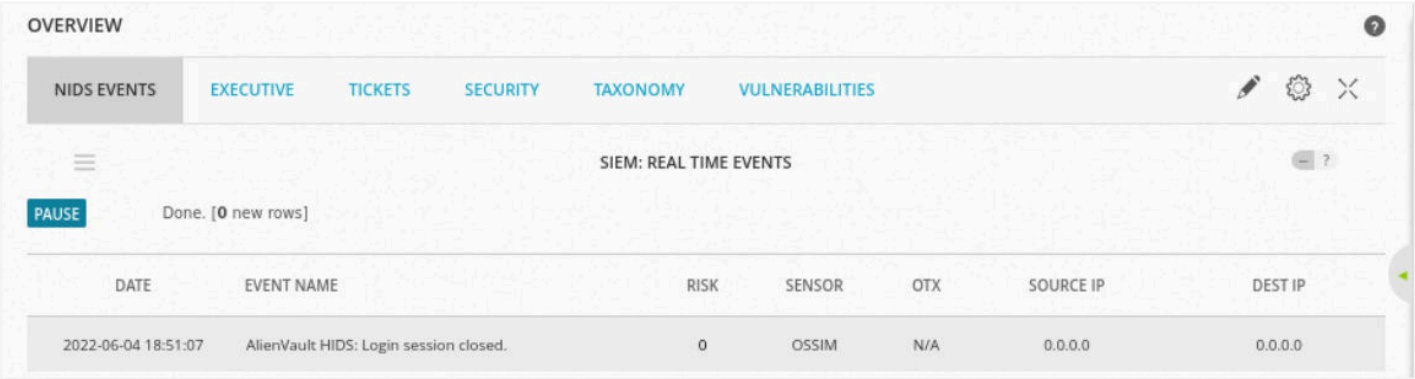


DATE	EVENT NAME	RISK	SENSOR	OTX	SOURCE IP	DEST IP
2022-06-04 13:46:28	SSHd: Connection closed	0	OSSIM	N/A	0.0.0.0:59632	0.0.0.0:22
2022-06-04 13:45:54	AlienVault HIDS: Login session opened.	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	AlienVault HIDS: Login session closed.	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	sudo: Session closed	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:54	sudo: Session closed	0	OSSIM	N/A	0.0.0.0	0.0.0.0
2022-06-04 13:45:53	sudo: Session opened	0	OSSIM	N/A	0.0.0.0	0.0.0.0

8. Finally, on the *Overview* page, click on the **here** link in the information box to return to View Mode.



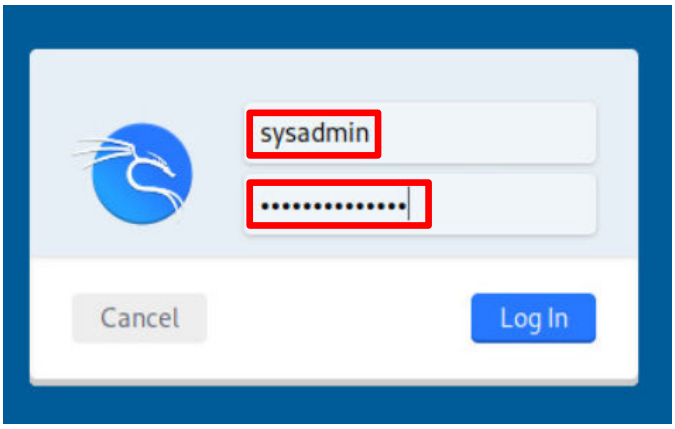
9. Remain on the *NIDS EVENTS* dashboard and continue to the next task.



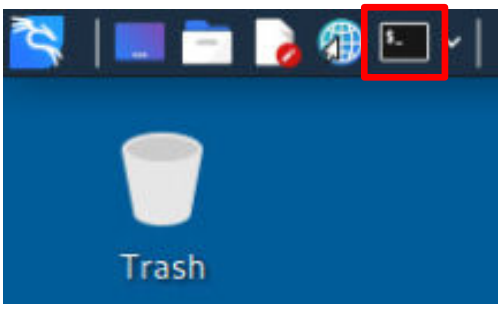
2.2 Generate Network Traffic to Produce NIDS Events

AlienVault OSSIM's NIDS function will constantly be monitoring and logging network traffic. In this task, you will be sending network traffic that will generate some NIDS events for analysis.

1. Set the focus on the **Kali** computer.
2. Log in as `sysadmin` using the password: `NDGlabpass123!`



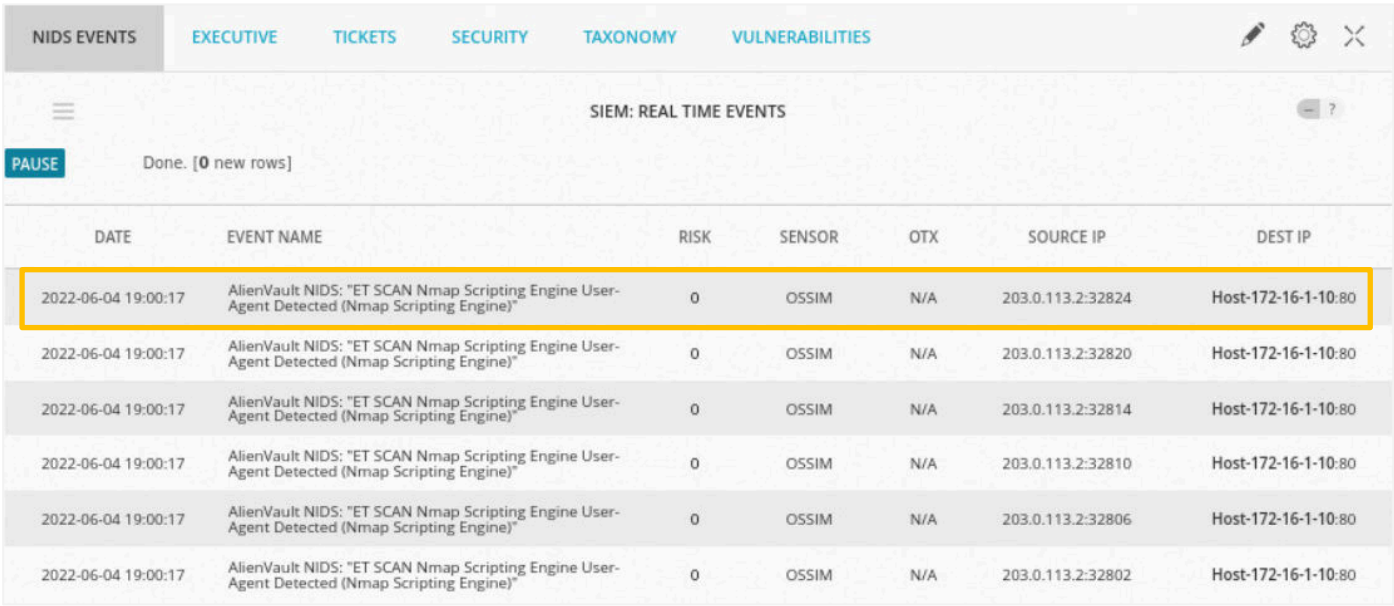
3. Click on the **Terminal** button.



4. In the terminal window, type the following to execute an *nmap* scan of the *UbuntuSRV* computer.

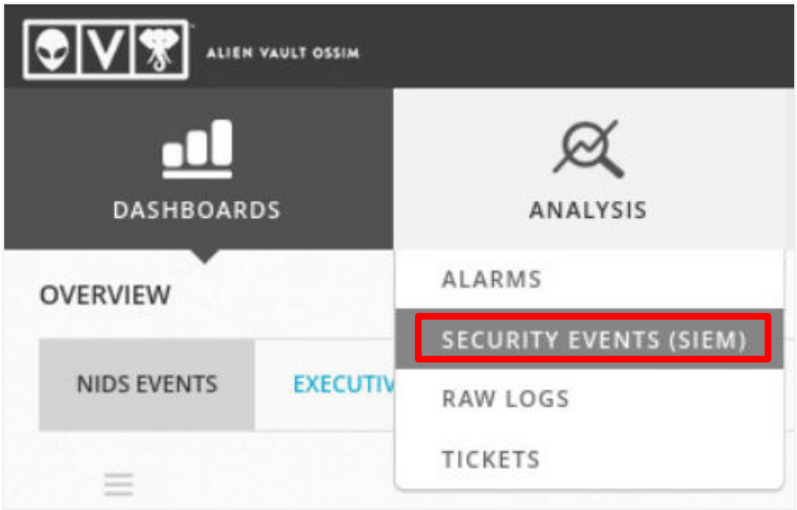
```
nmap -A 172.16.1.10
```

5. Set the focus on the **MintOS** computer and observe the *NIDS* events as they are collected and logged.

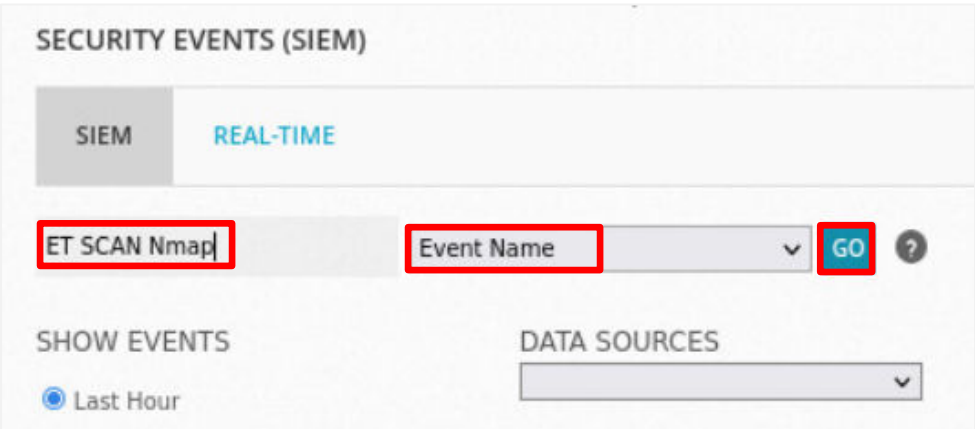


DATE	EVENT NAME	RISK	SENSOR	OTX	SOURCE IP	DEST IP
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32824	Host-172-16-1-10:80
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32820	Host-172-16-1-10:80
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32814	Host-172-16-1-10:80
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32810	Host-172-16-1-10:80
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32806	Host-172-16-1-10:80
2022-06-04 19:00:17	AlienVault NIDS: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"	0	OSSIM	N/A	203.0.113.2:32802	Host-172-16-1-10:80

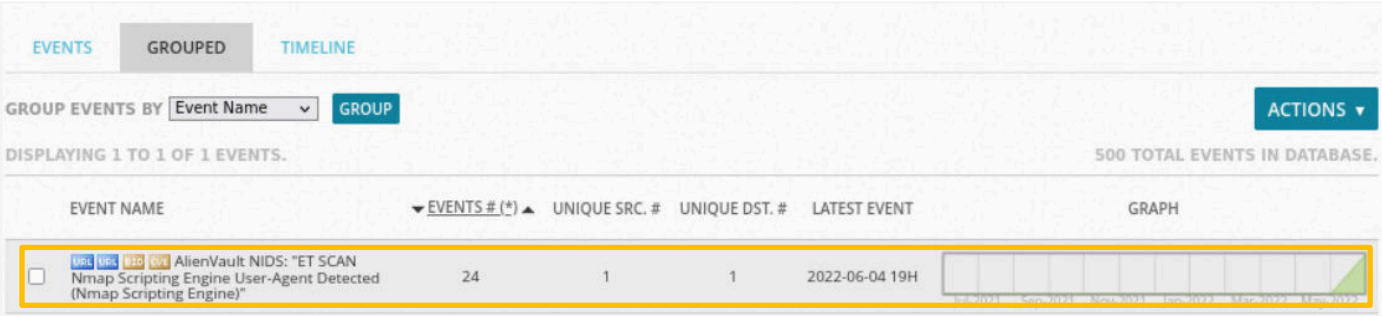
6. To examine the event in more detail, hover over the **ANALYSIS** menu item and then click on **SECURITY EVENTS (SIEM)**.



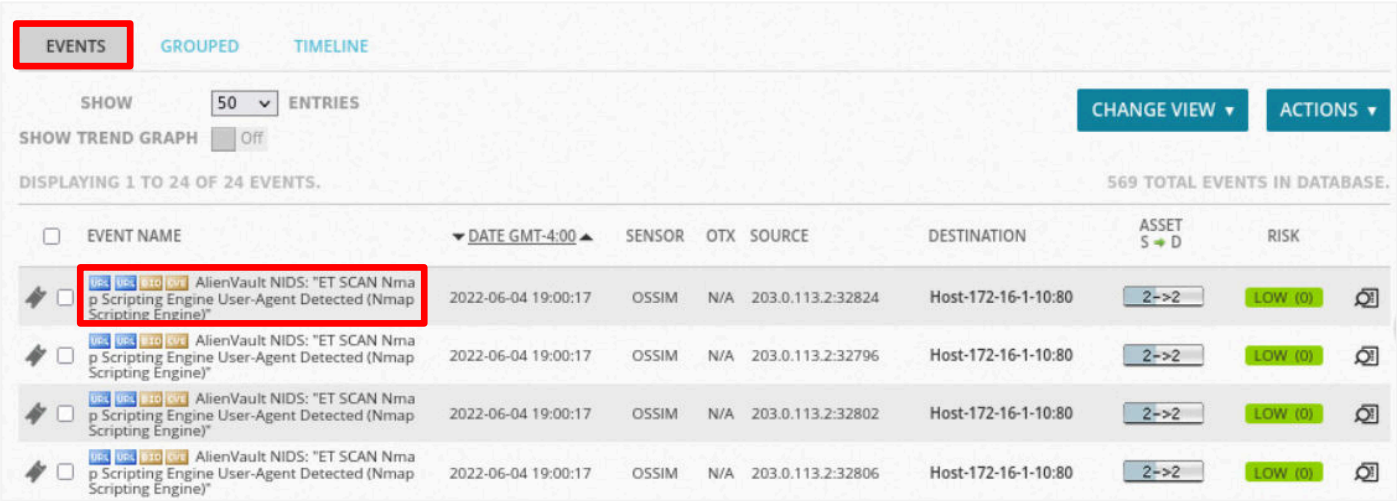
7. In order to find the events that were triggered by the *nmap* scan, type `ET SCAN Nmap` in the search box. Make sure **Event Name** is in the list box to the right and click the **GO** button.



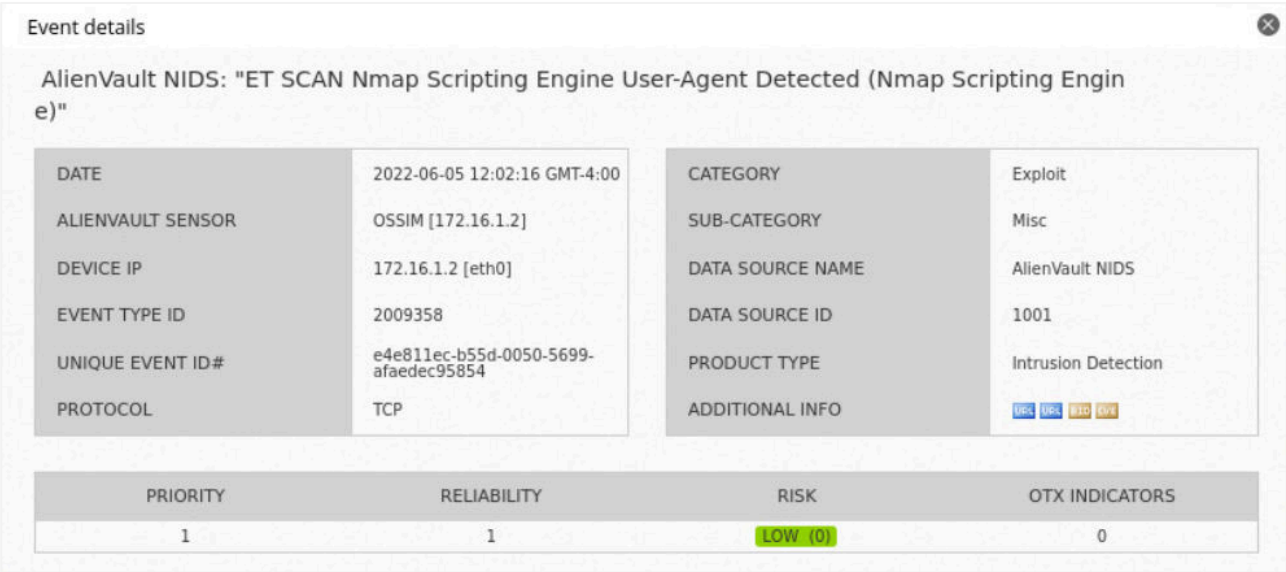
8. Scroll down the page, and you will see the *nmap* scan *Event* group.

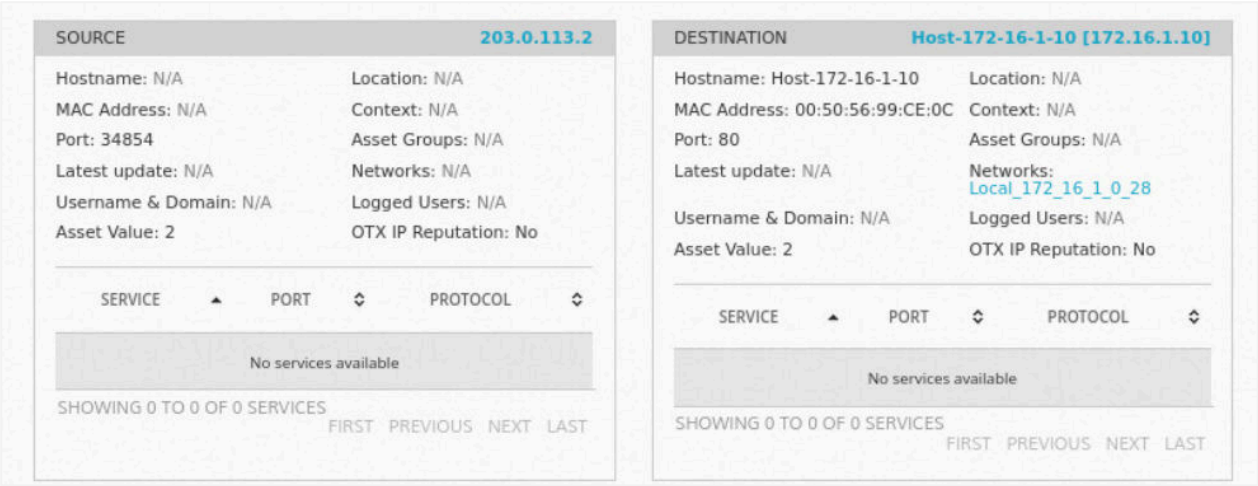


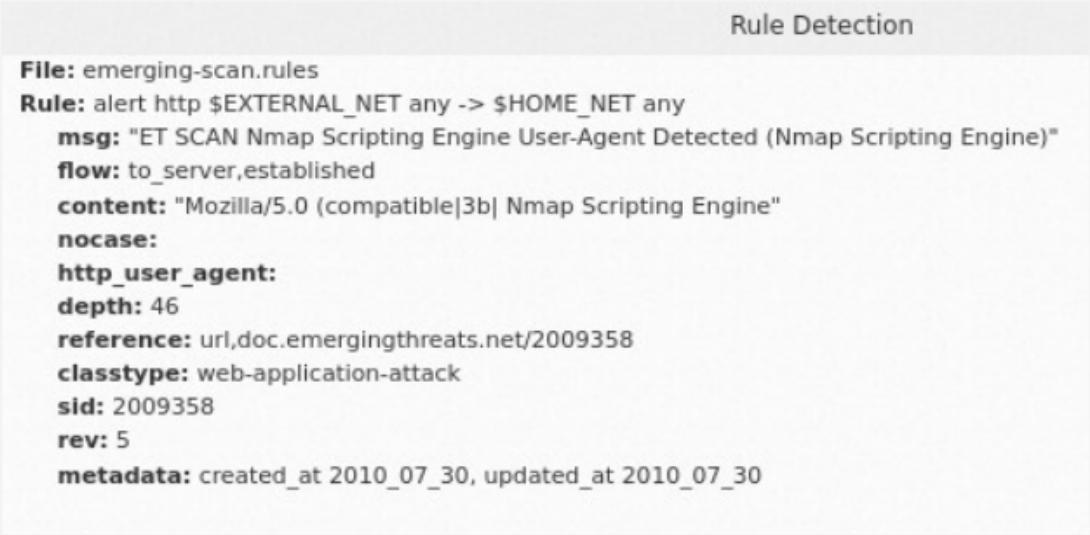
9. Click on the **EVENTS** menu tab to switch to the full list view of events. Click on the **first event** in the list to see the event details.



The *Event Details* window will show a very detailed view of the event, including the date/time of the event, the source IP information, the log, payload, and the rule that was used to detect and report the event.







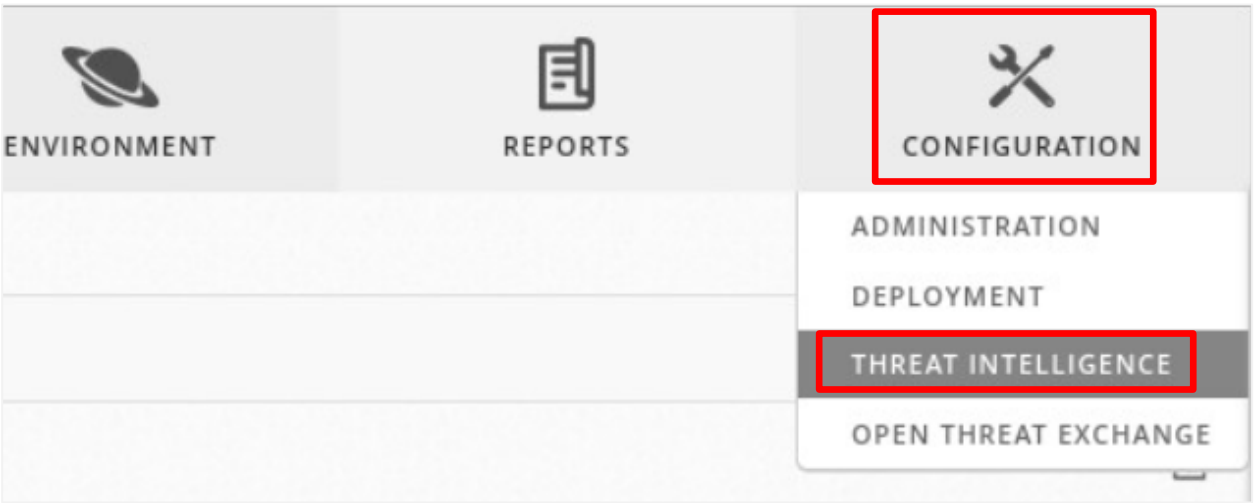
10. Click outside of the **Event Details** box to close the window.
11. Remain on the *AlienVault OSSIM* page on the *MintOS* computer and continue to the next task.

2.3 Rules and Correlation Directives

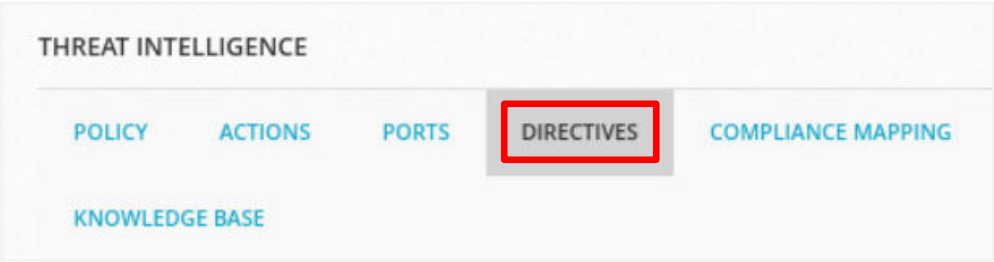
AlienVault OSSIM uses rules to correlate patterns of events to produce valuable information that a security analyst can use to detect various threats. One set of rules is supplied by a *Suricata* plugin called *AlienVault NIDS,* which is used to monitor promiscuous traffic delivered to *AlienValult OSSIM* and is matched again to threat signatures.

In this task, you will take a look at *Threat Intelligence Directives* (rules) that are used for monitoring and detecting malicious traffic.

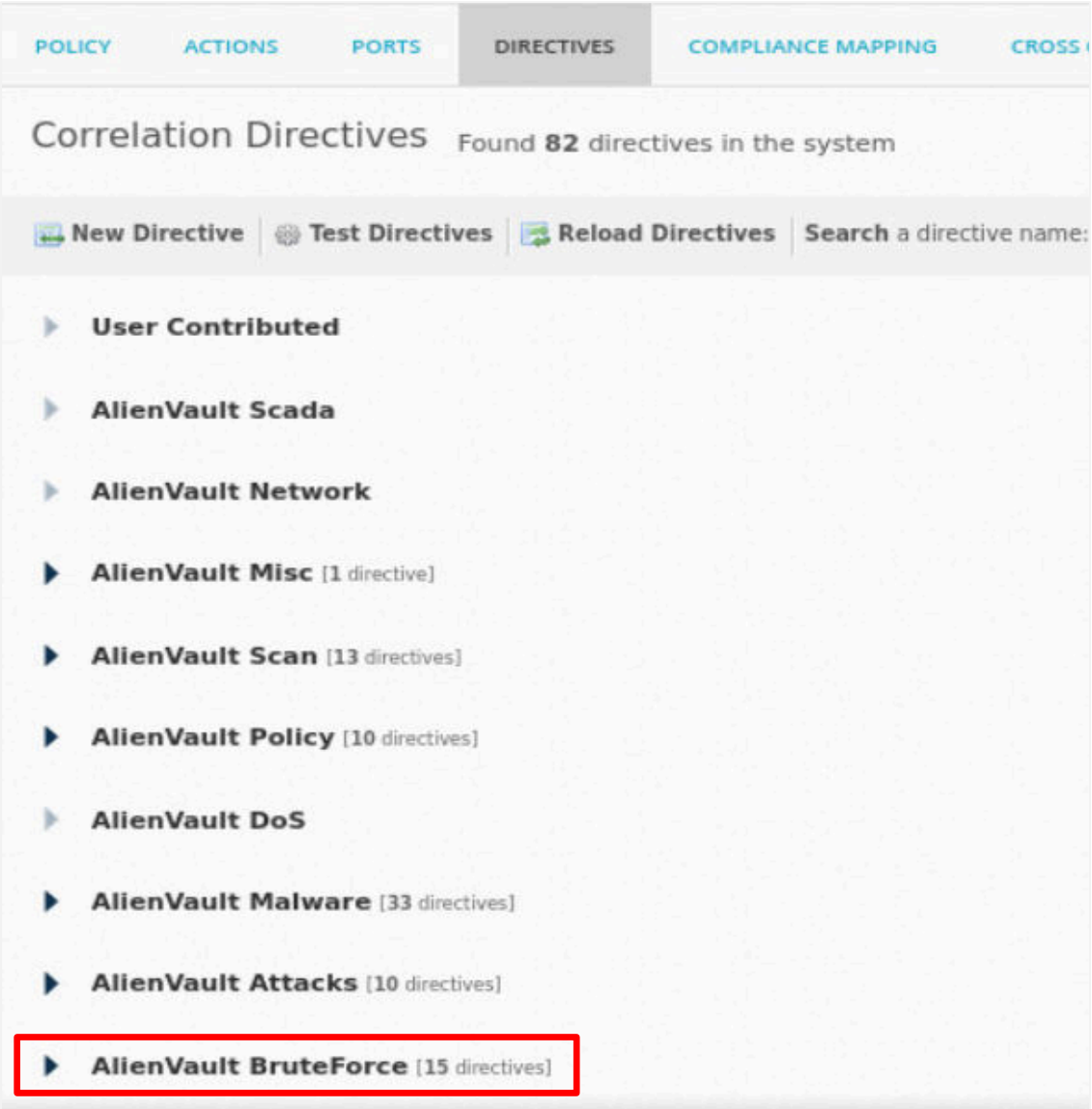
1. Hover over the **CONFIGURATION** button on the top menu and then click on **THREAT INTELLIGENCE.**



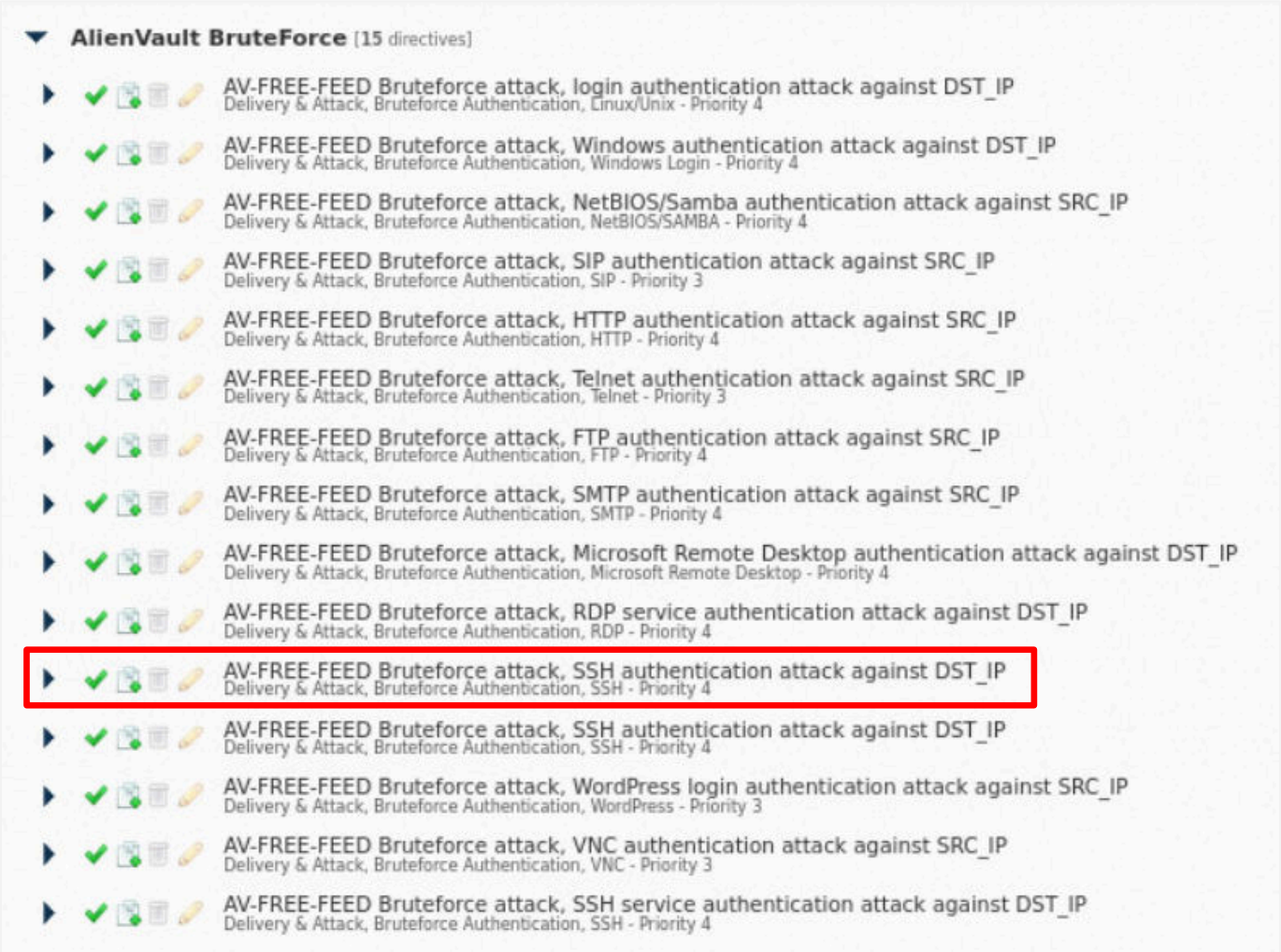
2. On the *THREAT INTELLIGENCE* page, click on **DIRECTIVES.**



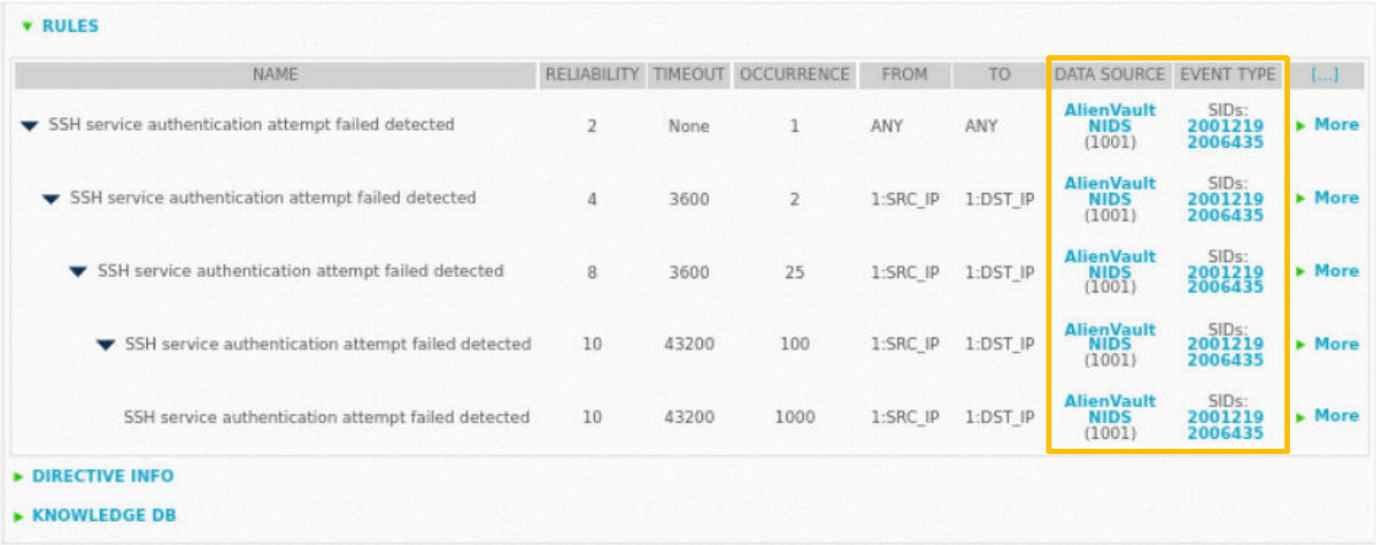
3. Under the *Correlation Directives* list, expand **AlienVault BruteForce.**



4. Scroll down the page and expand the first **AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP** directive.



5. In the *RULES* box, you will see a nested list of 5 rules, all showing *SSH service authentication attempt failed detected*.

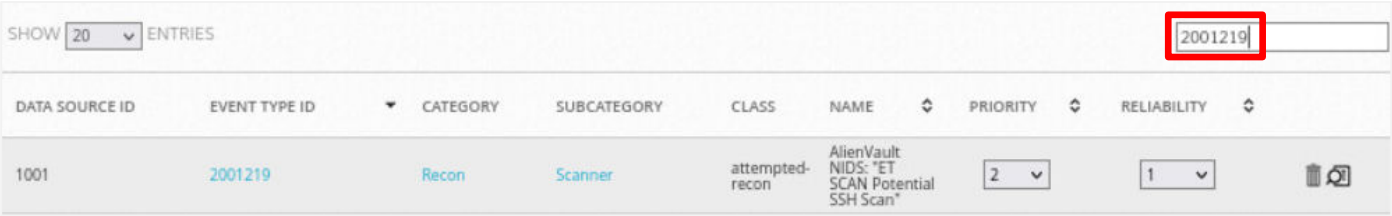


On the right side of the table, take note of the *DATA SOURCE*, showing that the rule source came from *AlienVault NIDS* (the *Suricata* plugin) and the *EVENT TYPE,* which shows two *SIDs* (Signature Identifiers) which are from the *Suricata* Rules.

6. Click on the first **AlienVault NIDS** link under *DATA SOURCE* to display the list of *SIDs* under *AlienVault NIDS* (Suracata) rules.

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE
SSH service authentication attempt failed detected	2	None	1	ANY	ANY	AlienVault NIDS (1001)	SIDs: 2001219 2006435

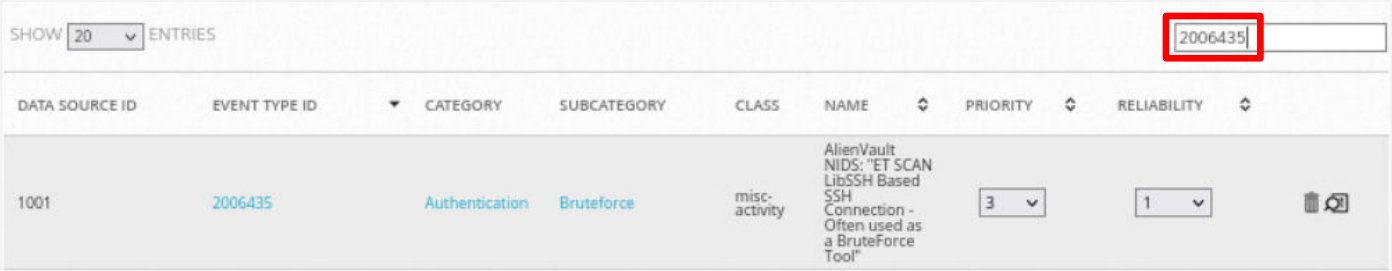
7. There are over 46,000 event types on the list. To display the *EVENT TYPE* for the *SSH Bruteforce* attack, type the first SID (**2001219**) from the *EVENT TYPE* column (shown above) into the **Search** box, and you should see the event information.



SHOW 20 ENTRIES 2001219

DATA SOURCE ID	EVENT TYPE ID	CATEGORY	SUBCATEGORY	CLASS	NAME	PRIORITY	RELIABILITY
1001	2001219	Recon	Scanner	attempted-recon	AlienVault NIDS: "ET SCAN Potential SSH Scan"	2	1

8. Repeat the search, this time using the second SID (**2006435**).



SHOW 20 ENTRIES 2006435

DATA SOURCE ID	EVENT TYPE ID	CATEGORY	SUBCATEGORY	CLASS	NAME	PRIORITY	RELIABILITY
1001	2006435	Authentication	Bruteforce	misc-activity	AlienVault NIDS: "ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool"	3	1

9. Set the focus on the **Kali** computer.
10. In the terminal, type the following command to start the *metasploit* process.
    If asked for the **[sudo] password for sysadmin**, use: `NDGlabpass123!`

```
sudo msfdb start
```

11. Run the **msfconsole**, with the following command:

```
msfconsole
```



```
┌──(sysadmin㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.1.38-dev                          ]
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 >
```

12. Type the following command to use the **SSH Login Scanner** module:

```
use auxiliary/scanner/ssh/ssh_login
```

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

13. Set the target IP address with the following command:

```
set RHOSTS 172.16.1.10
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.16.1.10
RHOSTS => 172.16.1.10
```

14. Set the username to root with the following command:

```
set USERNAME root
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME => root
```


15. Set the wordlist to use for the brute-force attack.

```
set PASS_FILE Desktop/LabFiles/HashCat/password.lst
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop/LabFiles/HashCat/password.lst
PASS_FILE => Desktop/LabFiles/HashCat/password.lst
```

16. Show results as *metasploit* brute-forces the password with the following command:

```
set VERBOSE true
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
```

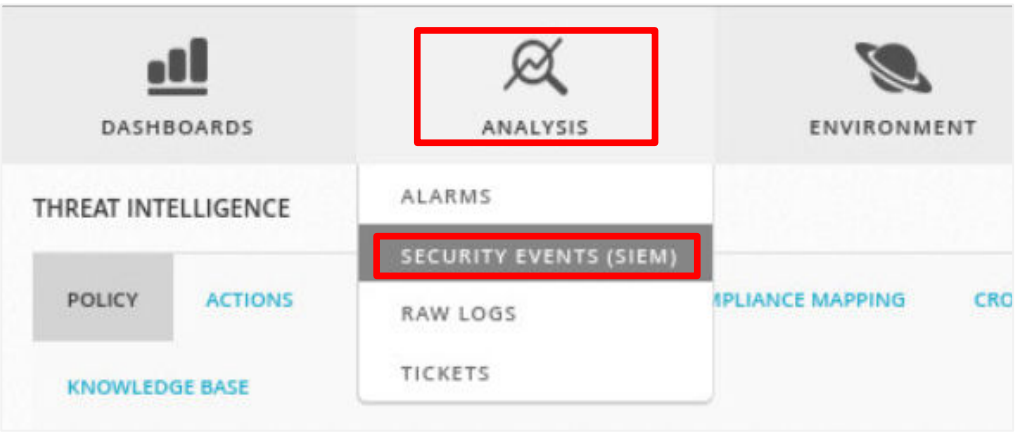
17. Start the attack with the **run** command:

```
run
```

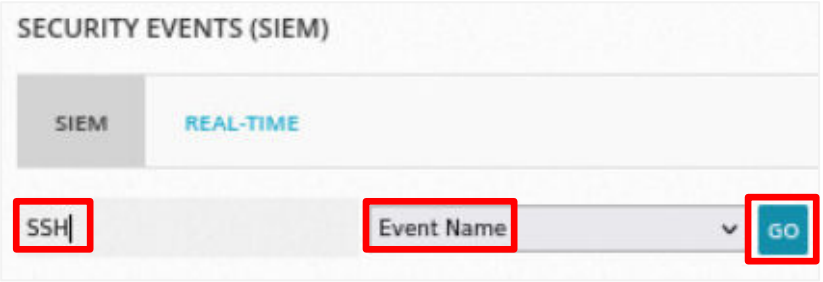
```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.16.1.10:22 - Starting bruteforce
[-] 172.16.1.10:22 - Failed: 'root:123456'
[!] No active DB -- Credential data will not be saved!
[-] 172.16.1.10:22 - Failed: 'root:12345'
[-] 172.16.1.10:22 - Failed: 'root:password'
[-] 172.16.1.10:22 - Failed: 'root:password1'
[-] 172.16.1.10:22 - Failed: 'root:123456789'
```

Allow the attack to run for at least 5-7 minutes to allow the directive to be detected before going on to the next step.

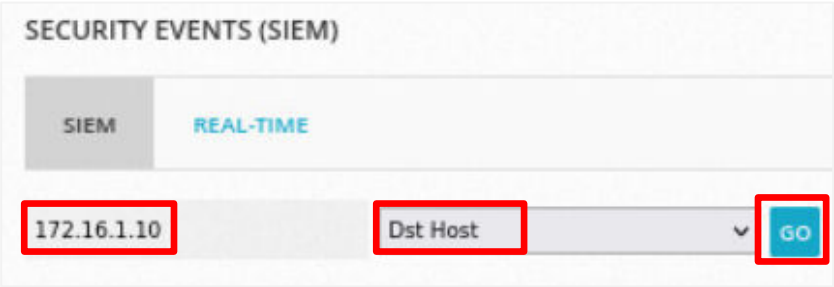
18. Return focus to the *MintOS* computer, hover over **ANALYSIS** and click on **SECURITY EVENTS (SIEM)**



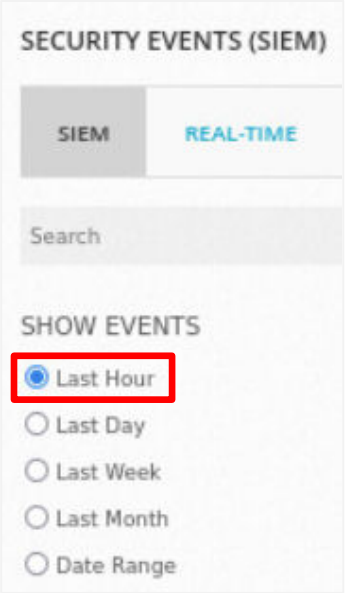
19. In the search box, type `SSH`, leave **Event Name** in the list box, and click **GO.**



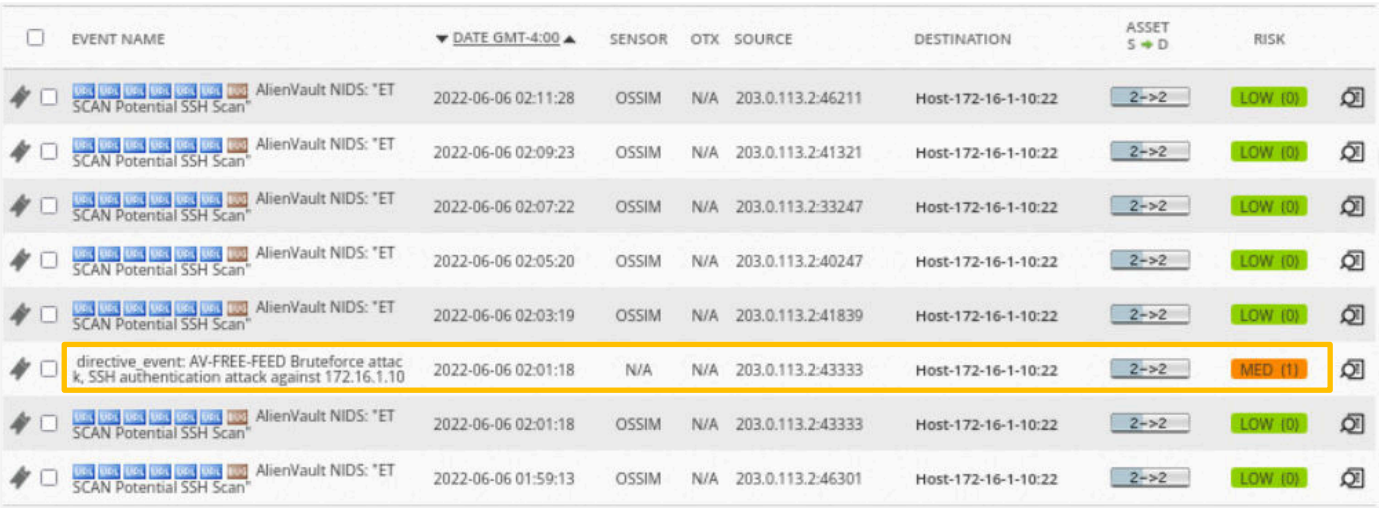
20. Add the *UbuntuSrv* computer to the search by typing `172.16.1.10` in the search box, use the list arrow to change the type to **Dst Host,** and click **GO.**



21. Under the *SHOW EVENTS* column, make sure the **Last Hour** is selected; if not, click on the **Last Hour** radio button.



22. Scroll down to the bottom of the page, and you will see all of the events that relate to SSH scans on the *UbuntuSRV* computer, including the *Directive Event* showing the authentication attack.

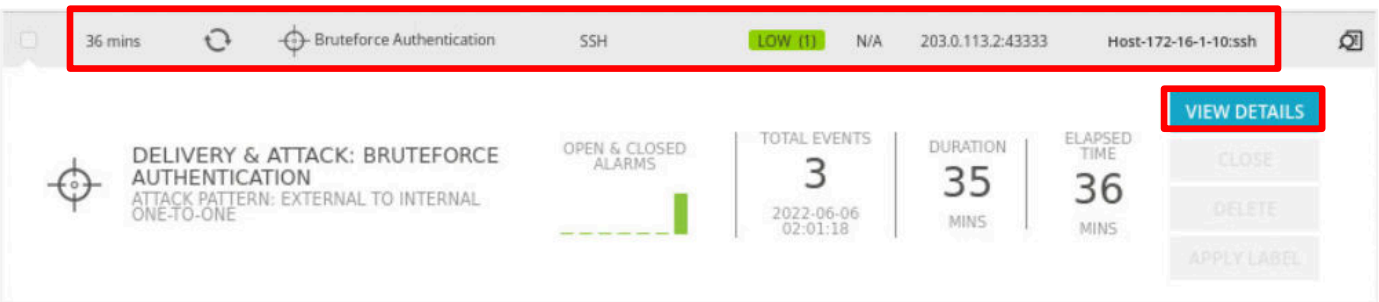


EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S→D	RISK
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:11:28	OSSIM	N/A	203.0.113.2:46211	Host-172-16-1-10:22	2->2	LOW (0)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:09:23	OSSIM	N/A	203.0.113.2:41321	Host-172-16-1-10:22	2->2	LOW (0)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:07:22	OSSIM	N/A	203.0.113.2:33247	Host-172-16-1-10:22	2->2	LOW (0)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:05:20	OSSIM	N/A	203.0.113.2:40247	Host-172-16-1-10:22	2->2	LOW (0)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:03:19	OSSIM	N/A	203.0.113.2:41839	Host-172-16-1-10:22	2->2	LOW (0)
directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against 172.16.1.10	2022-06-06 02:01:18	N/A	N/A	203.0.113.2:43333	Host-172-16-1-10:22	2->2	MED (1)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 02:01:18	OSSIM	N/A	203.0.113.2:43333	Host-172-16-1-10:22	2->2	LOW (0)
AlienVault NIDS: "ET SCAN Potential SSH Scan"	2022-06-06 01:59:13	OSSIM	N/A	203.0.113.2:46301	Host-172-16-1-10:22	2->2	LOW (0)

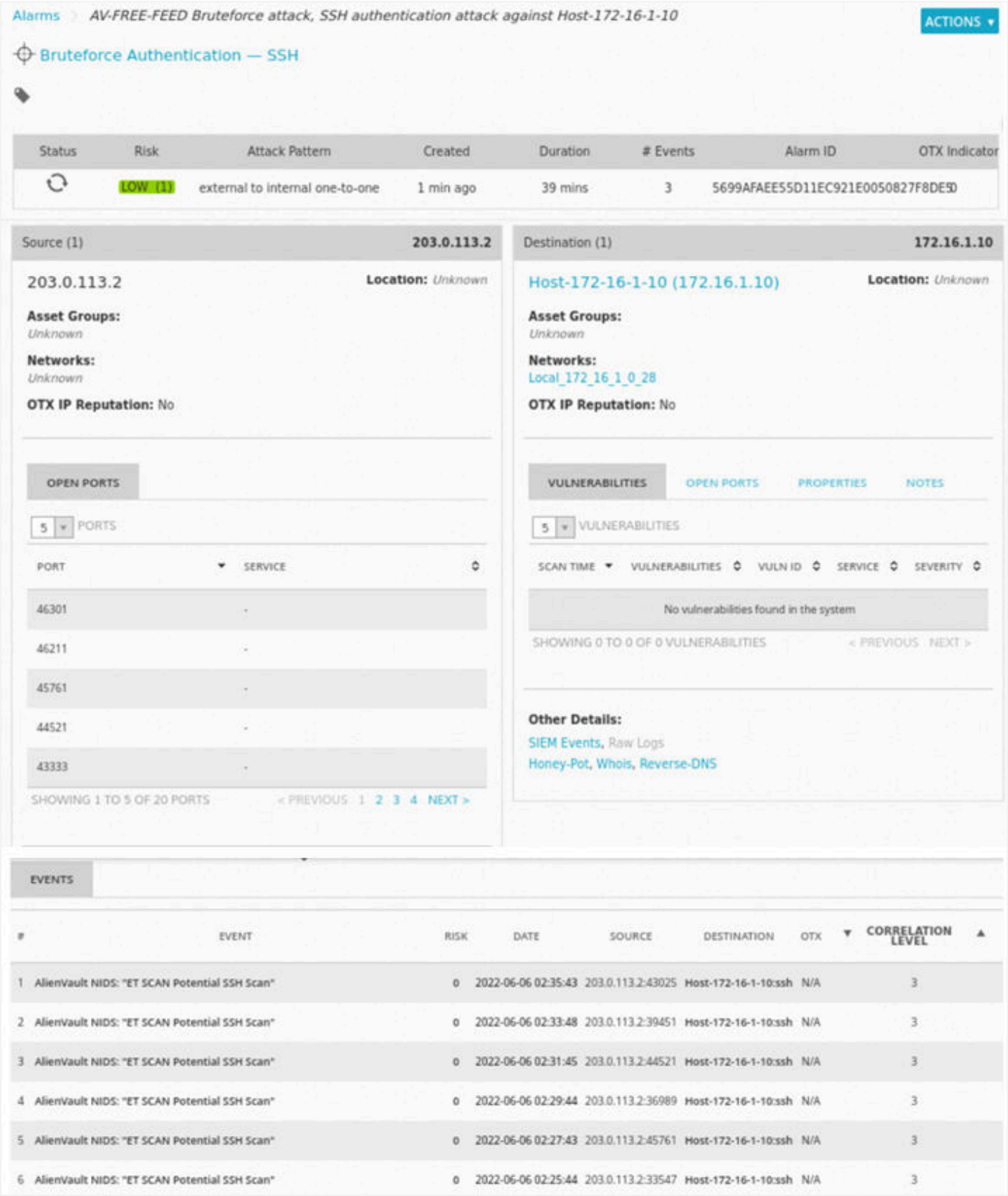
Notice that the event risk has a value of *(1)*, which will generate an alarm.

23. Hover back over the **ANALYSIS** button and click on **ALARMS**.

24. At the bottom of the page, you will see the *Bruteforce Authentication* alarm for *SSH*, including the source IP address where the attack came from. Click on the **alarm** to open a more detailed look.



25. Click on the **VIEW DETAILS** button to open the *Bruteforce Authentication – SSH* detail page.



26. Scroll down through the events and find the **AV-FREE-FEED Bruteforce Attack** event and click to open the *Event Detail* page.

#	EVENT	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	AV-FREE-FEED Bruteforce attack, SSH authentication attack against Host-172-16-1-10	1	2022-06-06 03:12:43	203.0.113.2:38817	Host-172-16-1-10:ssh	N/A	2

Alarm Summary [Total events matched with high rule level: 0 - Total Events: 2 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]

Event detail

directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against 172.16.1.10

DATE	2022-06-06 02:01:18 GMT-4:00	CATEGORY	Alarm
ALIENVAULT SENSOR	Unknown	SUB-CATEGORY	Bruteforce
DEVICE IP	N/A	DATA SOURCE NAME	directive_alert
EVENT TYPE ID	50098	DATA SOURCE ID	1505
UNIQUE EVENT ID#	5699afae-e55e-11ec-921e-005014ed8f46	PRODUCT TYPE	Alarm
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
4	4	MED (1)	0

SOURCE 203.0.113.2

Hostname: N/A
MAC Address: N/A
Port: 43333
Latest update: N/A
Username & Domain: N/A
Asset Value: 2
Location: N/A
Context: N/A
Asset Groups: N/A
Networks: N/A
Logged Users: N/A
OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES
FIRST PREVIOUS NEXT LAST

DESTINATION Host-172-16-1-10 [172.16.1.10]

Hostname: N/A
MAC Address: N/A
Port: 22
Latest update: N/A
Username & Domain: N/A
Asset Value: 2
Location: N/A
Context: N/A
Asset Groups: N/A
Networks: Local_172_16_1_0_28
Logged Users: N/A
OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES
FIRST PREVIOUS NEXT LAST

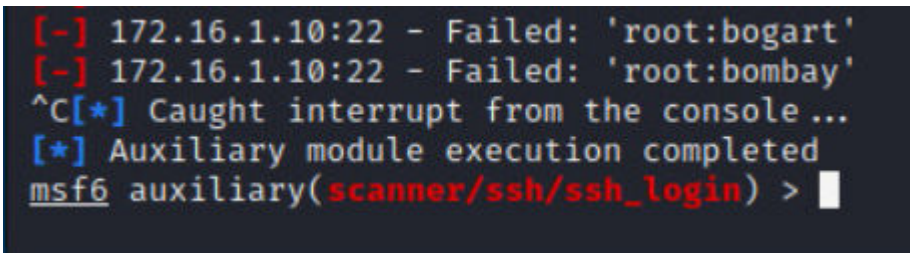
RAW LOG

```
directive_event: AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP, Prio
rity: 4 Rule 1 [2022-06-06 05:57:12]
[1001:2001219] [Rel: 2] 203.0.113.2:34653 -> 172.16.1.10:22 Rule 2 [2022-06-06 06:01:18] [1001:
2001219] [Rel: 4] 203.0.113.2:43333 ->
172.16.1.10:22
```


27. To assess the risk, use the following calculation:

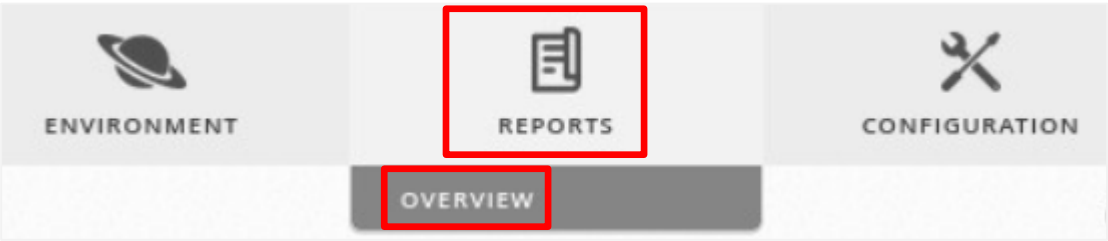
    Risk = int (Destination Asset Value * Priority * Reliability) / 25 … int (2 * 4 * 4) / 25 = int (1.28) = 1

28. Click on the **X** at the top of the *Event Detail* page to close the page.
29. Return the focus to the *Kali* computer and press **Ctrl+C** to stop the *SSH attack*.

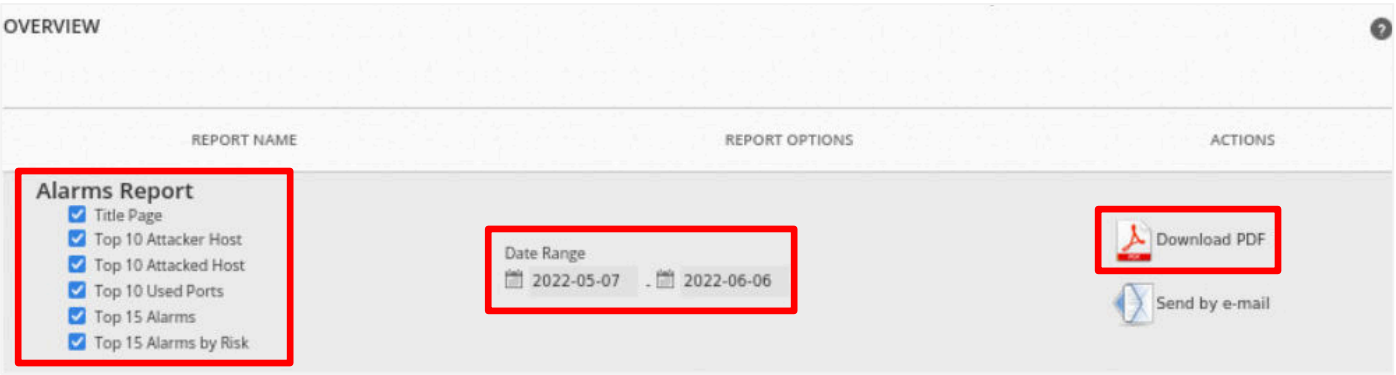


2.4 Compile and Generate NIDS Reports

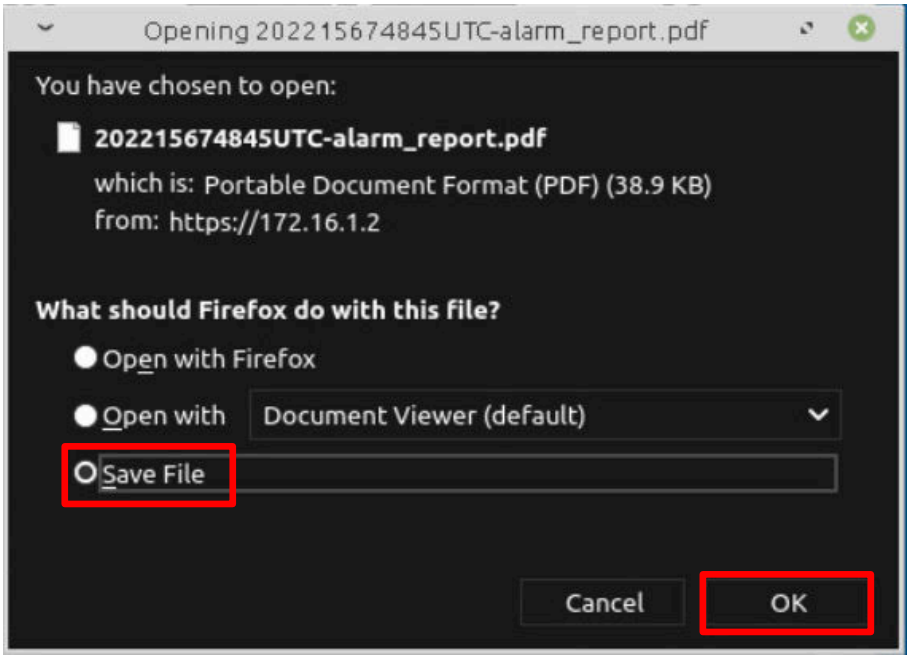
1. Set the focus to the *MintOS* computer.
2. Hover over the **REPORTS** button on the menu bar and click on **OVERVIEW**.



3. On the *OVERVIEW* page, you will generate an *Alarms Report*. Under *Alarms Report*, make sure all of the report pages are checked, and the date range shows a range that includes the current date. Click the **Download PDF** button.

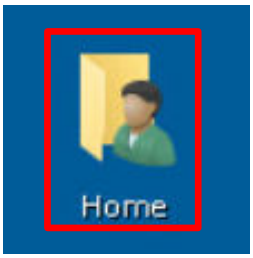


4. When the report is complete, make sure the **Save File** radio button is selected on the *What should Firefox do with this file?* popup window, and click the **OK** button.

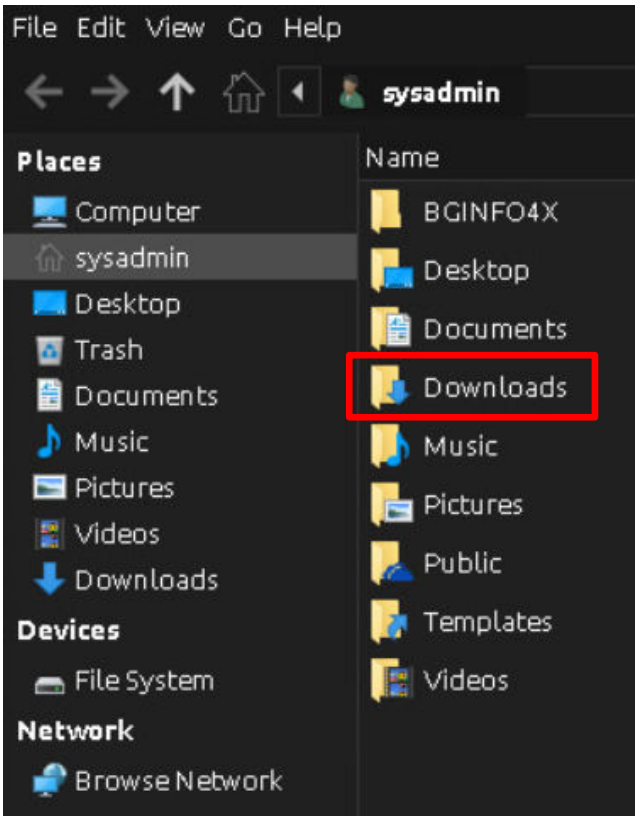


The file will be saved in the *Downloads* folder for the sysadmin user on the *MintOS* computer.

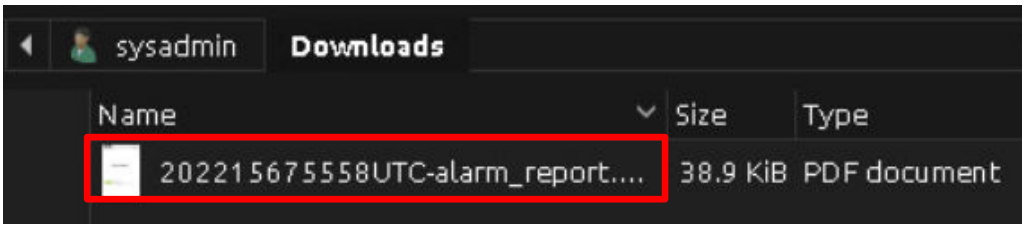
5. Close the web browser.
6. Double-click on the **Home** folder on the *MintOS* desktop.



7. In the *sysadmin* window, double-click on the **Downloads** folder.



8. In the *Downloads* folder, you should see the report that was just downloaded from *AlienVault OSSIM*. Double-click on the **file** to open it.



You will now see the Alarms Report that was just generated. This report can be used for further analysis.

9. The lab is now complete; you may now end the reservation.

