



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №8

Аналіз логів та робота з системою отримання інформації для розвідки кіберзагроз

Перевірив:

Козленко О. В.

Виконав:

студент IV курсу

групи ФБ-01

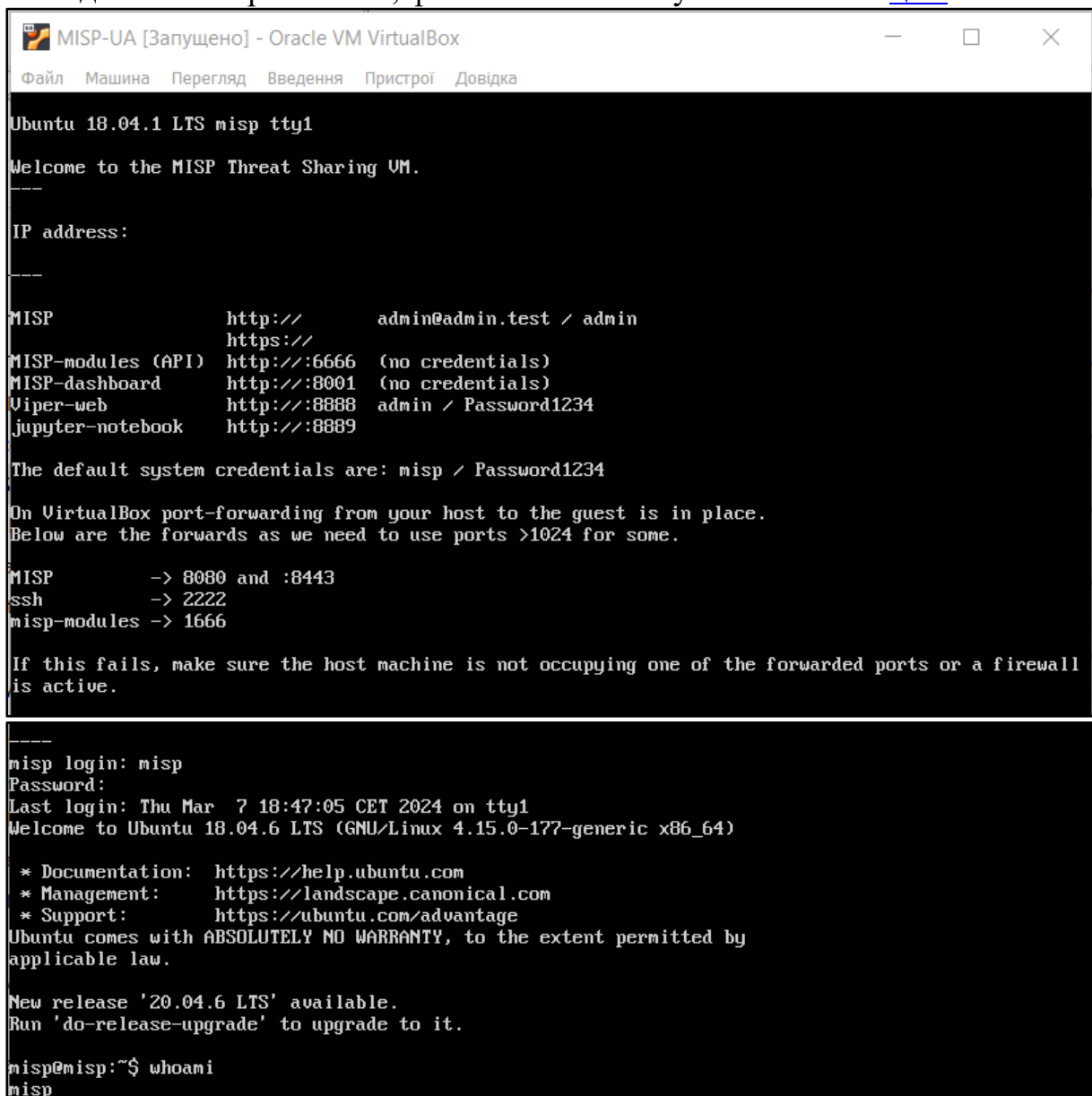
Сахній Н. Р.

Київ 2024

Мета: Отримати навички роботи з системою розповсюдження та створення інформації для використання у системах розвідки кіберзагроз та утилітою для аналізу логів web-сервера Apache.

Завдання: За допомогою системи [MISP](#) та тренувального набору даних отримати репорт щодо інцидентів у системі та зробити детальний аналіз лог-файлів Apache

1. Задеплоїмо сервіс MISP, файл OVA якого був скачаний за [цим](#) лінком:



```
MISP-UA [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Ubuntu 18.04.1 LTS misp tty1
Welcome to the MISP Threat Sharing VM.
---
IP address:
---
MISP                http://          admin@admin.test / admin
                    https://
MISP-modules (API)  http://:6666     (no credentials)
MISP-dashboard      http://:8001     (no credentials)
Viper-web           http://:8888     admin / Password1234
jupyter-notebook    http://:8889

The default system credentials are: misp / Password1234

On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.

MISP                -> 8080 and :8443
ssh                 -> 2222
misp-modules        -> 1666

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall
is active.

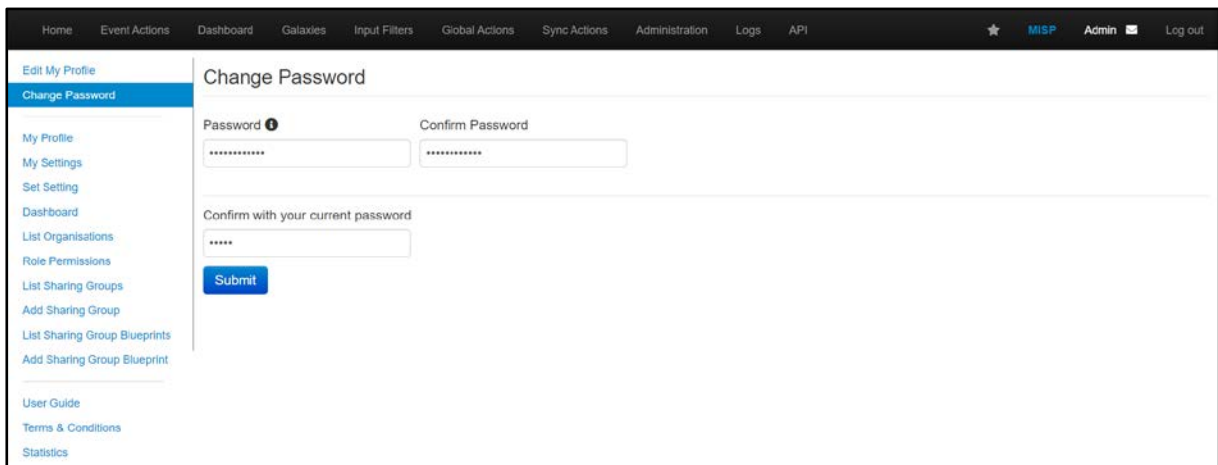
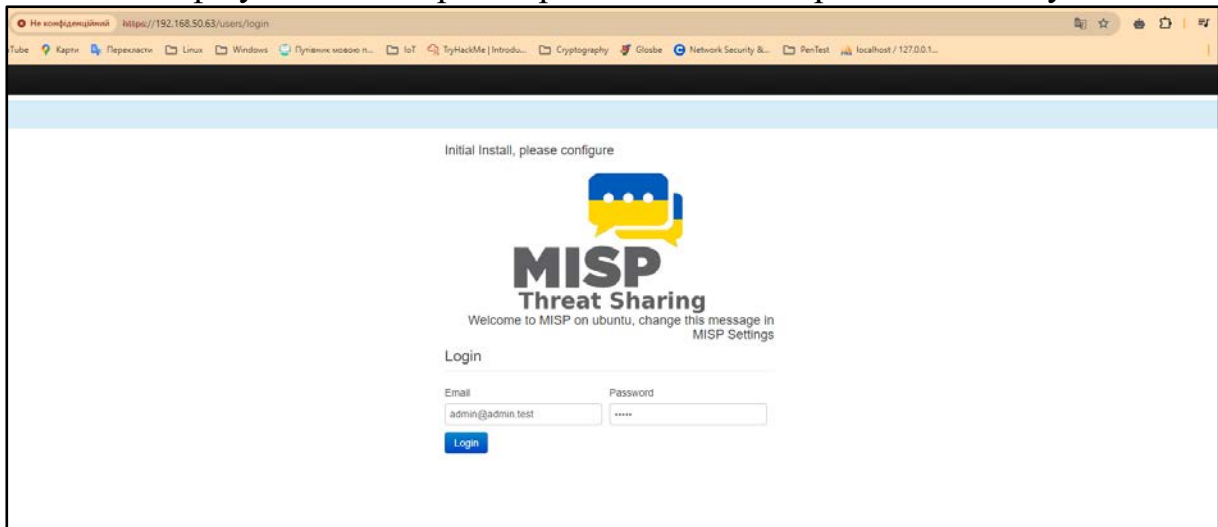
-----
misp login: misp
Password:
Last login: Thu Mar  7 18:47:05 CET 2024 on tty1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

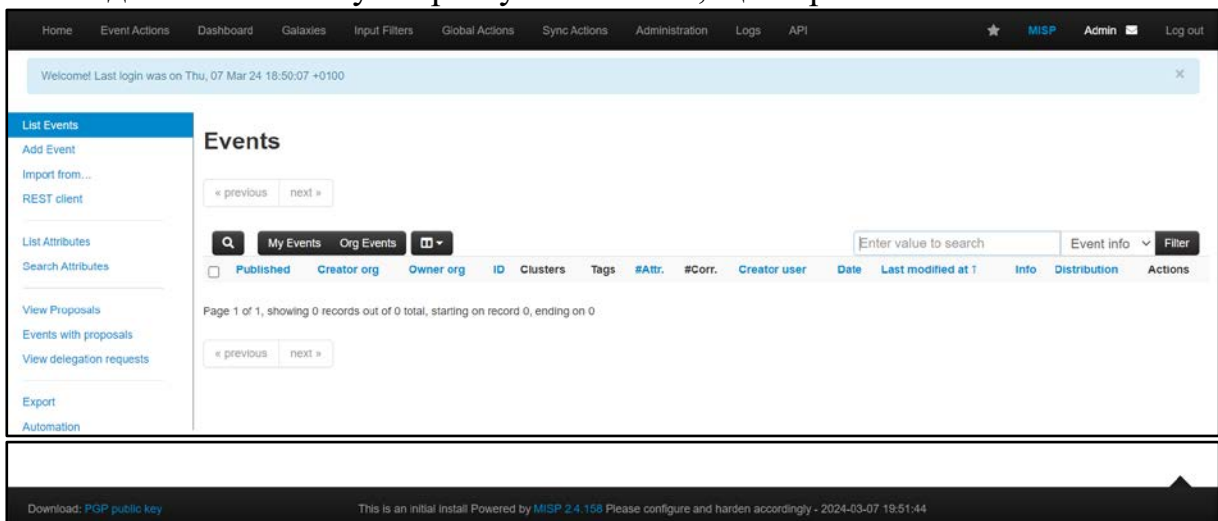
New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

misp@misp:~$ whoami
misp
```

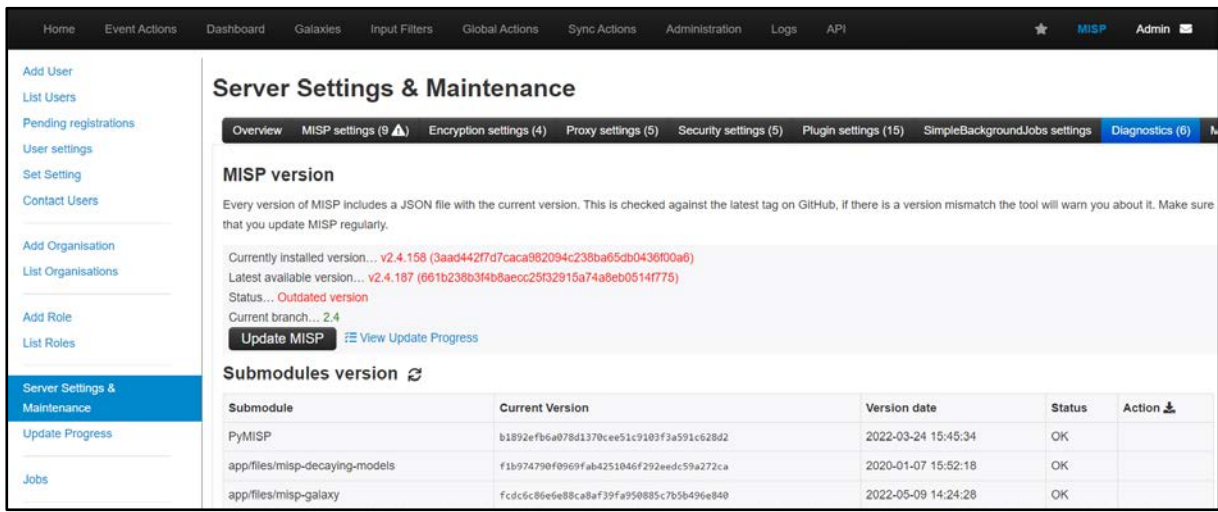
- Автентифікуємось та першочергово змінимо пароль за замовчуванням:



- Зайдемо на основну сторінку і помітимо, що наразі ніяких івентів немає:



- Оновимо версію MISP за URL-адресою /servers/serverSettings/diagnostics:



Server Settings & Maintenance

Overview MISP settings (9) Encryption settings (4) Proxy settings (5) Security settings (5) Plugin settings (15) SimpleBackgroundJobs settings Diagnostics (6)

MISP version

Every version of MISP includes a JSON file with the current version. This is checked against the latest tag on GitHub, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.158 (3aad442f7d7caca982094c238ba65db0436f00a6)
 Latest available version... v2.4.187 (661b238b3f4b8aecc25f32915a74a8eb0514f775)
 Status... **Outdated version**
 Current branch... 2.4

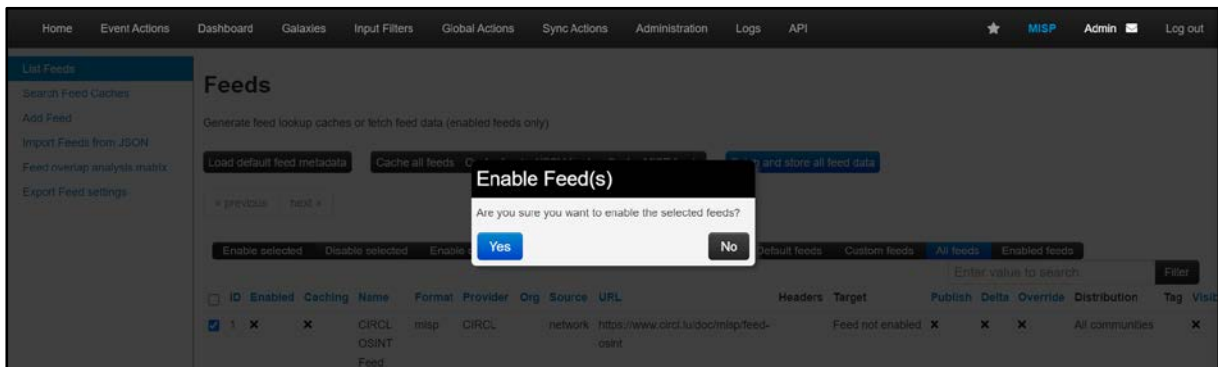
[Update MISP](#) [View Update Progress](#)

Submodules version

Submodule	Current Version	Version date	Status	Action
PyMISP	b1892efb6a078d1370cee51c9103f3a591c628d2	2022-03-24 15:45:34	OK	
app/files/misp-decaying-models	f1b974790f0969fab4251046f292eedc59a272ca	2020-01-07 15:52:18	OK	
app/files/misp-galaxy	fc0c6c86e6e88ca8af39fa950885c7b5b496e840	2022-05-09 14:24:28	OK	

Currently installed version... v2.4.187 (661b238b3f4b8aecc25f32915a74a8eb0514f775)
 Latest available version... v2.4.187 (661b238b3f4b8aecc25f32915a74a8eb0514f775)
 Status... OK
 Current branch...

- Законектимо доступний канал даних CIRCL OSINT Feed (/feeds/index):



Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

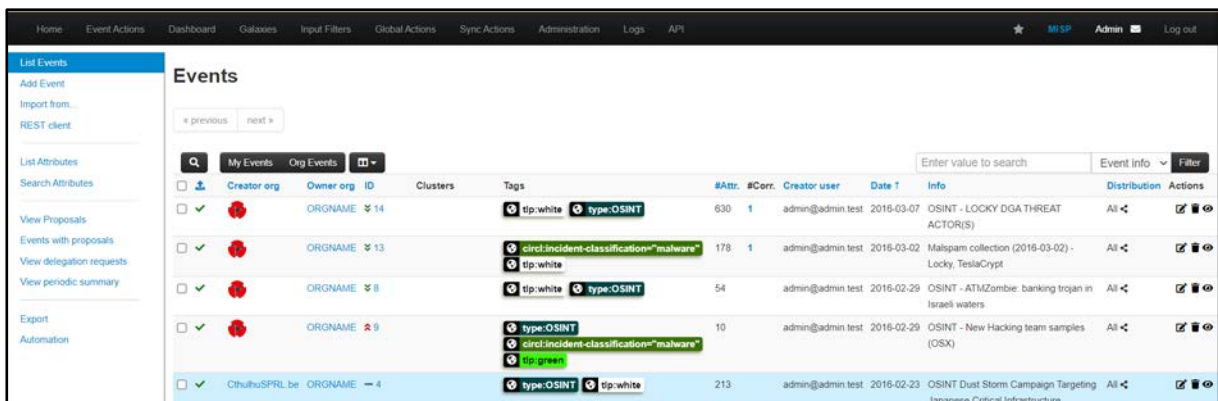
Load default feed metadata Cache all feeds Fetch feed data and store all feed data

Are you sure you want to enable the selected feeds?

Yes No

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Vis
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT Feed	misp	CIRCL	network	https://www.circl.lu/doc/misp/feed-osint			Feed not enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All communities		<input checked="" type="checkbox"/>

- Тепер ми можемо помітити, що вже стали підвантажились івенти із ІоС:



Events

My Events Org Events

ID	Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Info	Distribution	Actions
<input checked="" type="checkbox"/>	ORNAME	ORNAME	14		tip:white type:OSINT	630	1	admin@admin test	2016-03-07	OSINT - LOCKY DGA THREAT ACTOR(S)	All	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ORNAME	ORNAME	13		circular:incident-classification=malware tip:white	178	1	admin@admin test	2016-03-02	Malspam collection (2016-03-02) - Locky, TeslaCrypt	All	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ORNAME	ORNAME	8		tip:white type:OSINT	54		admin@admin test	2016-02-29	OSINT - ATMZombie: banking trojan in Israeli waters	All	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ORNAME	ORNAME	9		type:OSINT circular:incident-classification=malware tip:green	10		admin@admin test	2016-02-29	OSINT - New Hacking team samples (OSX)	All	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Citihub/SPRL.be	ORNAME	4		type:OSINT tip:white	213		admin@admin test	2016-02-23	OSINT Dust Storm Campaign Targeting Japanese Critical Infrastructure	All	<input checked="" type="checkbox"/>

- Переглянемо звіт про атаку “Guccifer 2.0: All Roads Lead to Russia”:

The screenshot shows the MISP (Malware Information Sharing Platform) interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. A message at the top states: "You are currently logged in as a site administrator and about to edit an event not belonging to your organisation. This goes against the sharing model of MISP. Use a normal user account for day to day work."

The left sidebar contains a "View Event" section with options: View Correlation Graph, View Event History, Edit Event, Delete Event, Add Attribute, Add Object, Add Attachment, Add Event Report, Populate from..., Enrich Event, Merge attributes from..., Unpublish, Publish Sightings, Download as..., Add Event to Collection, List Events, and Add Event.

The main content area displays the event details for "Guccifer 2.0: All Roads Lead to Russia - Threatconnect report". The event ID is 184. The UUID is 5797c2d2-5784-4ab9-b6c7-4e98960d210f. The creator org is CIRCL, and the owner org is ORGNAME. The creator user is admin@admin.test. The event is in unprotected mode. The tags are ttp:white, type:OSINT, and type:ATTACK. The date is 2016-07-26, and the threat level is High. The analysis is Ongoing. The distribution is All communities. The event is published (Yes) on 2024-03-07 20:18:46. It has 11 attributes. The first recorded change is on 2016-07-26 22:20:25, and the last change is on 2016-07-26 22:21:44. The modification map shows a single change. The event has 0 sightings, restricted to own organisation only.

At the bottom, there are tabs for: —Pivots, —Galaxy, —Event graph, —Event timeline, —Correlation graph, —ATT&CK matrix, —Event reports, —Attributes, and —Discussion.

- Помітимо, що присутні ІоС, які мають негативну репутацію. Далі можна перейти до етапу їх блокування на мережевому обладнанні (фаєрволах):

<div> + - Scope toggle Deleted Decay score Context Related Tags Filtering tool </div>										
<input type="checkbox"/>	Date	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
<input type="checkbox"/>	2016-07-26	579...10f	External analysis	link	https://www.threatconnect.com/guccifer-2-all-roads-lead-russia/			Original report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	domain	xocma.net			Imported via the Freetext Import Tool	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.38			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.40			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.41			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	hostname	fr1.vpn-service.us			Imported via the Freetext Import Tool	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Payload delivery	email-src	sec.service@mail.ru			Imported via the Freetext Import Tool	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.34			Original IP of the email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.9.198			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.36			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2016-07-26	579...10f	Network activity	ip-dst	95.130.15.37			Same SSH fingerprint as 95.130.15.34	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Page 1 of 1, showing 1 records out of 11 total, starting on record 1, ending on 11

[previous](#)
[next](#)
[view all](#)

The screenshot shows the VirusShare interface. On the left, there is a circular progress indicator showing a score of 1/91. Below it, a "Community Score" section shows a score of 100%.

The main content area displays the domain "xocma.net". A warning icon and text state: "1/91 security vendor flagged this domain as malicious". Below the domain name, there are tabs for "media sharing" and "top-100K".

On the right, there are three columns of information:

- Registrar: OnlineNIC, Inc.
- Creation Date: 22 years ago
- Last Analysis Date: 6 months ago

At the bottom right, there are icons for "Similar", "Graph", and "API".

2. Проаналізуємо access.log файл, який ми ще розглядали на Advanced SQL:

	A	B	C	D	E	F	G	H
1	ID	Line						
2	1	13.66.139.0 - - [19/Dec/2020:13:57:26 +0100] "GET /index.php?option=com_phocagallery&view=category&id=1:almhuette-raith&Itemid=53 HTTP/1.1" 200 32653 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.101 Safari/537.36"						
3	2	157.48.153.185 - - [19/Dec/2020:14:08:06 +0100] "GET /apache-log/access.log HTTP/1.1" 200 233 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.101 Safari/537.36"						
4	3	157.48.153.185 - - [19/Dec/2020:14:08:08 +0100] "GET /favicon.ico HTTP/1.1" 404 217 "http://www.almhuette-raith.at/apache-log/access.log" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.101 Safari/537.36"						
5	4	216.244.66.230 - - [19/Dec/2020:14:14:26 +0100] "GET /robots.txt HTTP/1.1" 200 304 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot/faq)"						
6	5	54.36.148.92 - - [19/Dec/2020:14:16:44 +0100] "GET /index.php?option=com_phocagallery&view=category&id=2%3Awinterfotos&Itemid=53 HTTP/1.1" 200 30662 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.101 Safari/537.36"						

- Згенеруємо доступний та інтерактивний звіт за допомогою GoAccess:

```
(root@snz24)-[/home/nazar/Стільниця]
# goaccess -f access.log > /var/www/html/access.log.html
[PARSING access.log] {94,228} @ {47,114/s}
```

