Cyber Security

Class no 05(Lab 3, Arabi Sir)

21 Sep 2024

# Reconnaissance:

- OSINT – Open Source Intelligence

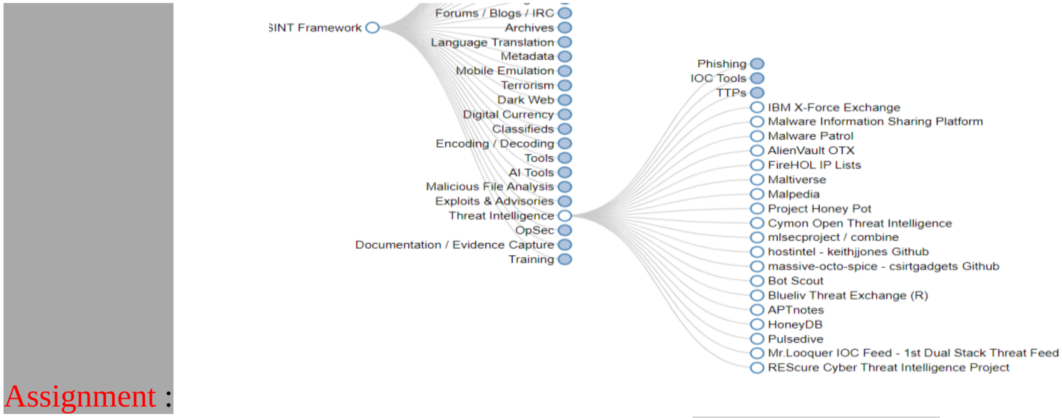
Pentest Methodology

- https://www.virustotal.com/gui/ → check is there any virus in crack file→ for any link must first try this link and then click the link
- https://app.any.run/ →virus check for file
- https://leakpeek.com/ → check, is your data public?
- For a picture, first check property
- How to create a Share Folder in kali Linux →See assignment
    - First turnoff the virtual machine then start again
    - Cd /media/sf_JU →sf mean shared file //terminal (use TAB button)
    - Store ch9 file in shared folder manually
    - Disk file check →testdisk ch9 →Intel→advance→FAT32 →list→file→if there is a red file then go this file using cursor and type C and again C… file will be store in JU folder→convert file into ZIP →then extract all→check properties of this picture →
    - Terminal → cd /media/sf_JU/Files/revendications/Pictures →file location
        - Type exiftool 1000000000.jpg →picture name → show all details about this picture
        - https://www.gps-coordinates.net/ → add coordinate

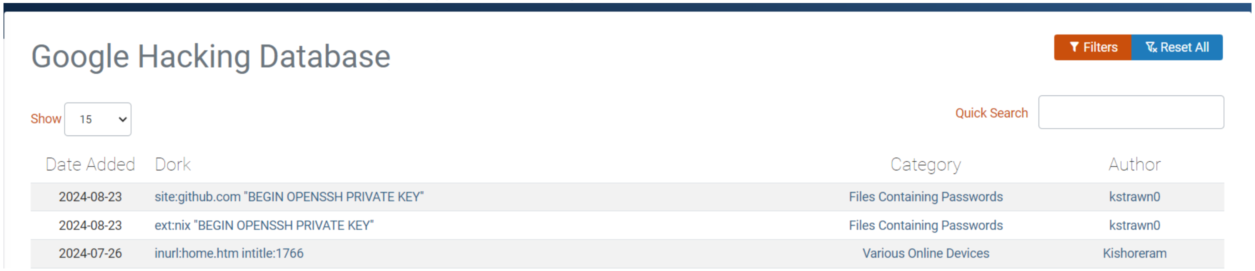
```
┌──(shariful㉿kali)-[~]

└─$ sudo -i

[sudo] password for shariful:

┌──(root㉿kali)-[~]

└─# cd /media/sf_Share

┌──(root㉿kali)-[/media/sf_Share]

└─# ls

ch9
```

```
┌──(root㉿kali)-[/media/sf_Share]
└─# testdisk ch9
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

┌──(root㉿kali)-[~]
└─# cd /media/sf_Share/Files/revendications/Pictures        (Use TAB)

┌──(root㉿kali)-[/media/sf_Share/Files/revendications/Pictures]
└─# exiftool 1000000000000CC000000990038D2A62.jpg
```

- https://osintframework.com/ →Check fast



- Assignment :
- Exodus mobile aps: → for check any aps permission. Very important aps
- https://osintleak.com/dashboard : **for user all details**
- ?intitle:index.of? pdf hacking → for download any file/videos/ or goto https://www.dorkgpt.com/
  site:juniv.edu filetype:doc
- dorkgpt. Com theke j kono 5 ta search er assignment
- https://www.exploit-db.com/google-hacking-database → Exploit database

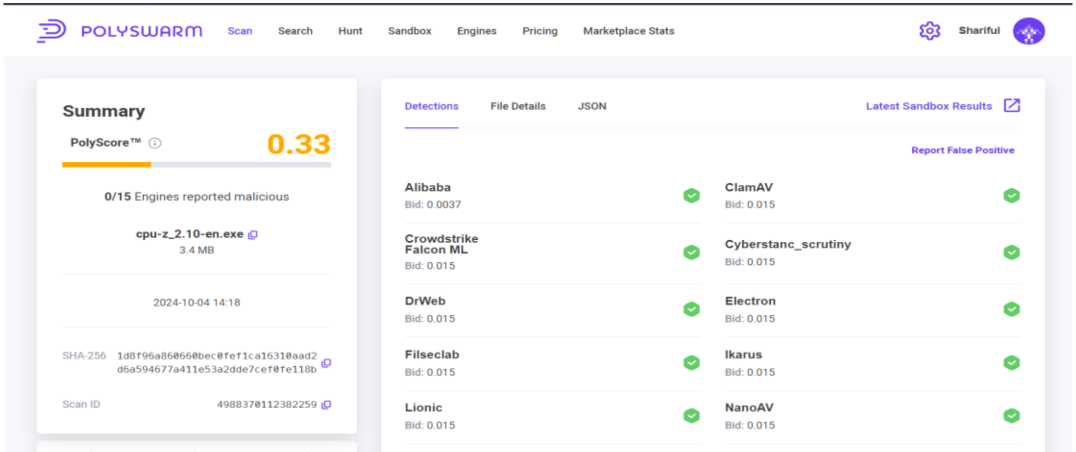


Google Hacking Database

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram

- https://polyswarm.io/

Scan for big data/file



Summary

PolyScore™ 0.33

0/15 Engines reported malicious

cpu-z_2.10-en.exe
3.4 MB

2024-10-04 14:18

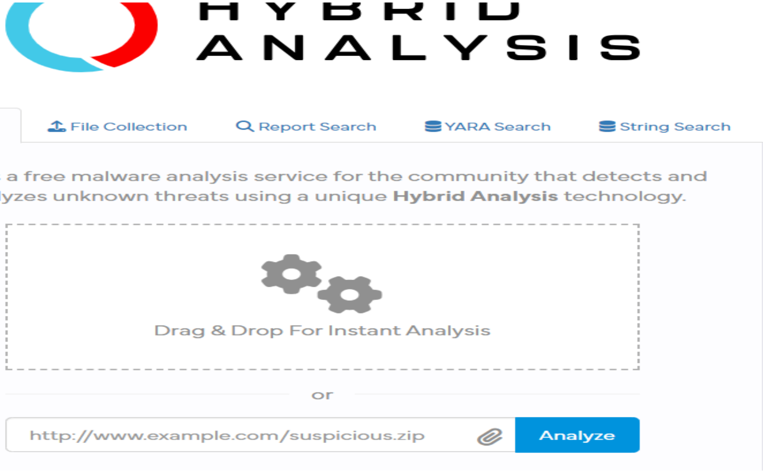
SHA-256 1d8f96a860660bec0fef1ca16310aad2d6a594677a411e53a2dde7cef0fe118b

Scan ID 4988370112382259

Alibaba Bid: 0.0037	✓	ClamAV Bid: 0.015	✓
Crowdstrike Falcon ML Bid: 0.015	✓	Cyberstanc_scrutiny Bid: 0.015	✓
DrWeb Bid: 0.015	✓	Electron Bid: 0.015	✓
Filseclab Bid: 0.015	✓	Ikarus Bid: 0.015	✓
Lionic Bid: 0.015	✓	NanoAV Bid: 0.015	✓

- https://www.hybrid-analysis.com/

Free automated malware analysis

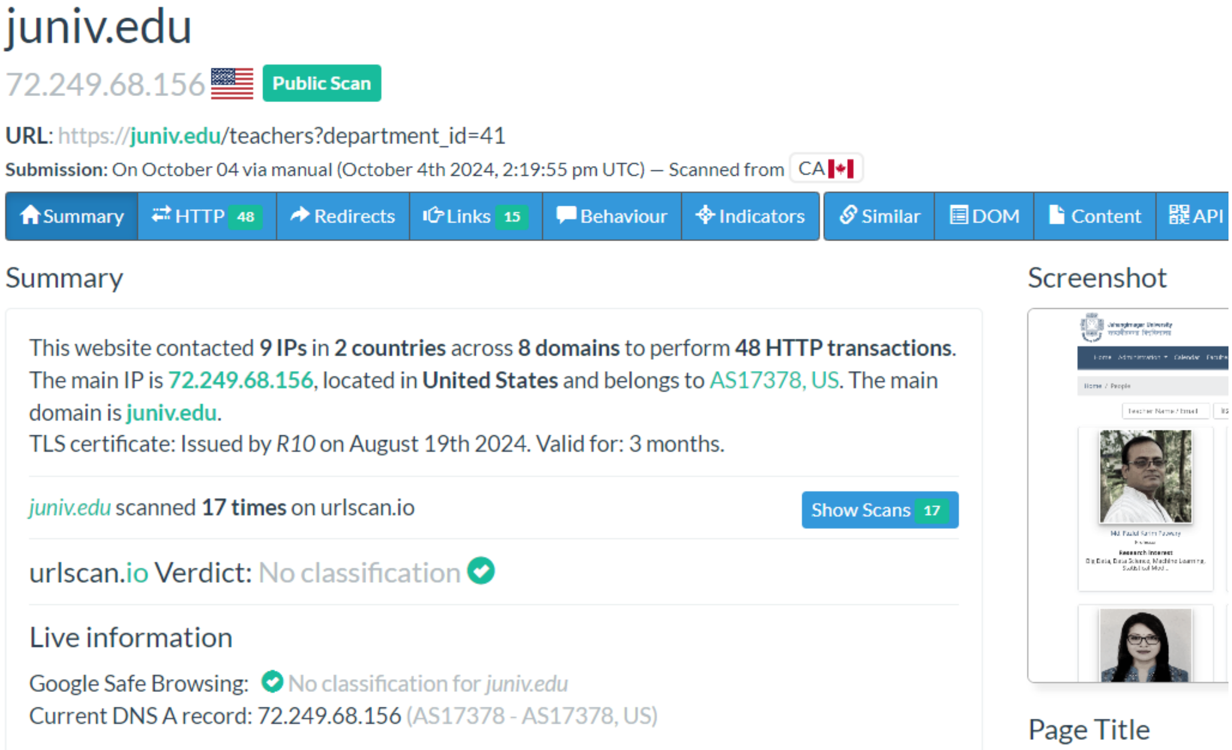


This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Drag & Drop For Instant Analysis
or
http://www.example.com/suspicious.zip
Analyze

- https://urlscan.io/

Domain and IP information and all details about any URL



juniv.edu

72.249.68.156 Public Scan

URL: https://**juniv.edu**/teachers?department_id=41

Submission: On October 04 via manual (October 4th 2024, 2:19:55 pm UTC) — Scanned from CA

Summary

This website contacted **9 IPs** in **2 countries** across **8 domains** to perform **48 HTTP transactions**. The main IP is **72.249.68.156**, located in **United States** and belongs to **AS17378, US**. The main domain is **juniv.edu**.
TLS certificate: Issued by *R10* on August 19th 2024. Valid for: 3 months.

juniv.edu scanned **17 times** on urlscan.io

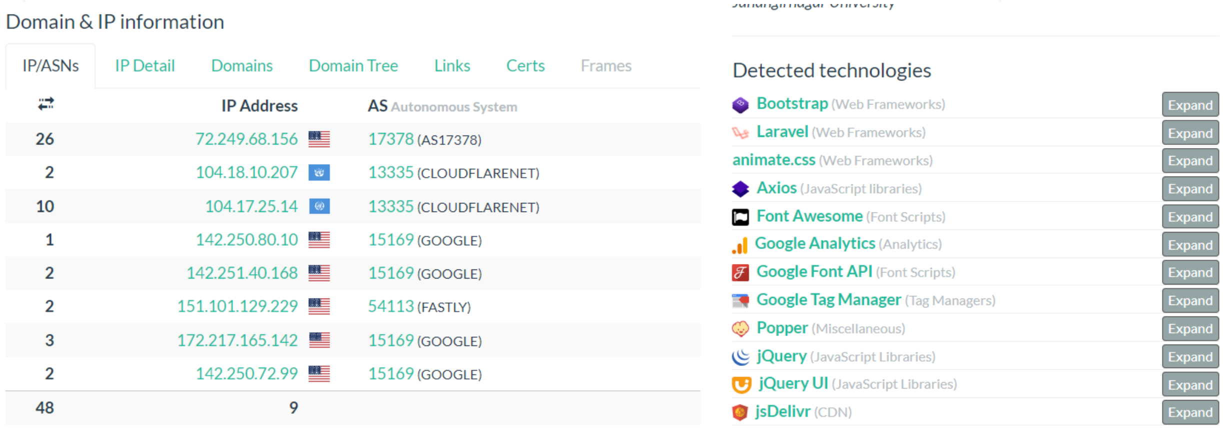
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *juniv.edu*
Current DNS A record: 72.249.68.156 (AS17378 - AS17378, US)

Screenshot

Page Title



Jahangirnagar University

Domain & IP information

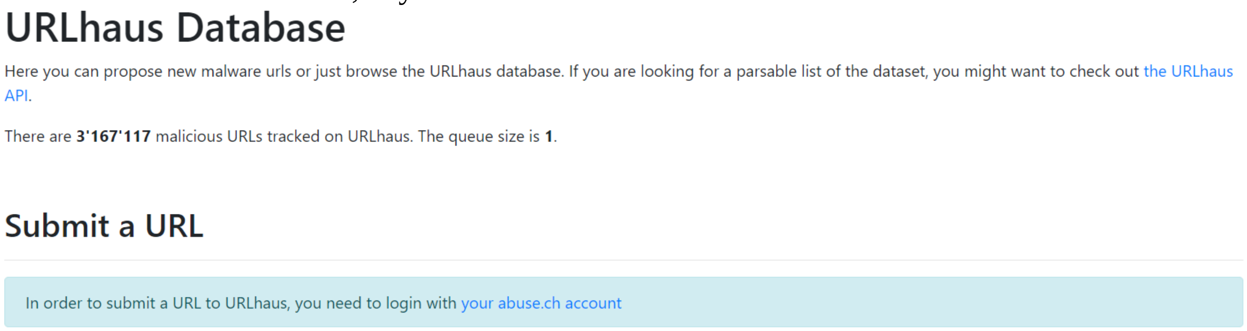
⇄	IP Address	AS Autonomous System
26	72.249.68.156	17378 (AS17378)
2	104.18.10.207	13335 (CLOUDFLARENET)
10	104.17.25.14	13335 (CLOUDFLARENET)
1	142.250.80.10	15169 (GOOGLE)
2	142.251.40.168	15169 (GOOGLE)
2	151.101.129.229	54113 (FASTLY)
3	172.217.165.142	15169 (GOOGLE)
2	142.250.72.99	15169 (GOOGLE)
48	9	

Detected technologies

Bootstrap (Web Frameworks) Expand
Laravel (Web Frameworks) Expand
animate.css (Web Frameworks) Expand
Axios (JavaScript libraries) Expand
Font Awesome (Font Scripts) Expand
Google Analytics (Analytics) Expand
Google Font API (Font Scripts) Expand
Google Tag Manager (Tag Managers) Expand
Popper (Miscellaneous) Expand
jQuery (JavaScript Libraries) Expand
jQuery UI (JavaScript Libraries) Expand
jsDelivr (CDN) Expand

- https://talosintelligence.com/
- https://urlhaus.abuse.ch/browse/

List of all malware website, anyone can submit a website as a malware.



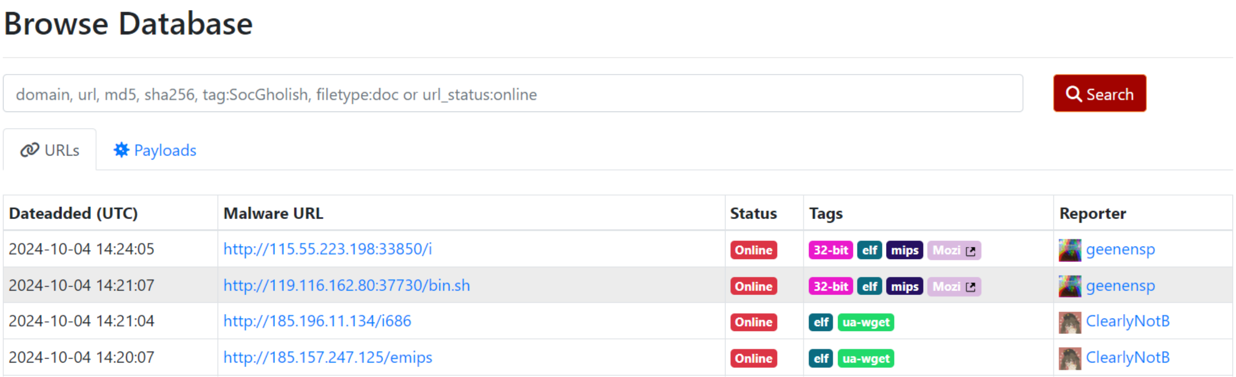
URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out the URLhaus API.

There are **3'167'117** malicious URLs tracked on URLhaus. The queue size is **1**.

Submit a URL

In order to submit a URL to URLhaus, you need to login with your abuse.ch account

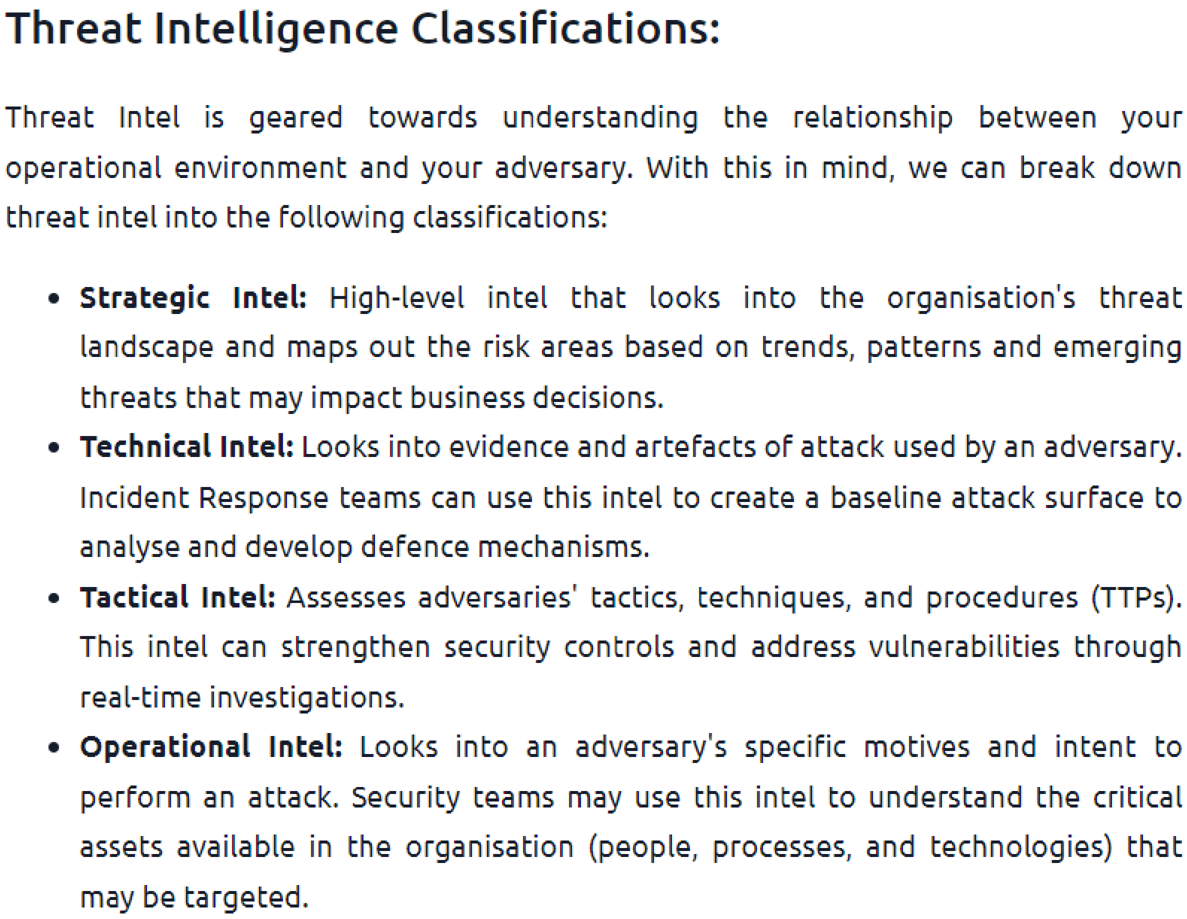


Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2024-10-04 14:24:05	http://115.55.223.198:33850/i	Online	32-bit elf mips Mozi	geenensp
2024-10-04 14:21:07	http://119.116.162.80:37730/bin.sh	Online	32-bit elf mips Mozi	geenensp
2024-10-04 14:21:04	http://185.196.11.134/i686	Online	elf ua-wget	ClearlyNotB
2024-10-04 14:20:07	http://185.157.247.125/emips	Online	elf ua-wget	ClearlyNotB

-
- Assignment: world wide CC tv access



Threat Intelligence Classifications:

Threat Intel is geared towards understanding the relationship between your operational environment and your adversary. With this in mind, we can break down threat intel into the following classifications:

- **Strategic Intel:** High-level intel that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.
- **Technical Intel:** Looks into evidence and artefacts of attack used by an adversary. Incident Response teams can use this intel to create a baseline attack surface to analyse and develop defence mechanisms.
- **Tactical Intel:** Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.
- **Operational Intel:** Looks into an adversary's specific motives and intent to perform an attack. Security teams may use this intel to understand the critical assets available in the organisation (people, processes, and technologies) that may be targeted.

-
- https://abuse.ch/ → check 6 category assignment

# Link from Arabi Sir:

https://polyswarm.network/scan

https://metadefenderopswat.com/

https://analyze.intezer.com/

https://www.hybrid-analysis.com/

https://app.any.run/

https://tria.ge/submit/file

OSINT Tools Collections #1

OSRFramework: https://lnkd.in/dY2TZARX

OSINTLeaks: https://osintleak.com/

ChatGPT like web:

1. Poe
2. https://claude.ai/new
3.

Just search and see:

- intitle:"webcamxp 5"
- site:juniv.edu filetype:pdf
- http://insecam.org/en/byrating/
-