OPEN-SOURCE INTELLIGENCE

WHAT DOES OPEN-SOURCE MEAN?

It means Publicly available.

(FREE)

OSINT can help in threat intelligence, identifying vulnerabilities, and more.

WHAT DOES INTELLIGENCE MEAN?

Analyzing the information gathered to obtain a full and better picture.

WHAT IS CYBER THREAT INTELLIGENCE?

CTI is defined as the collection and analysis of information about threats and adversaries and drawing patterns that provide an ability to make knowledgeable decisions for the preparedness, prevention, and response actions against various cyber-attacks.

IMPORTANCE OF CTI

- sheds light on the unknown, enabling security teams to make better decisions
- revealing adversarial motives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor’s decision-making process
- empowers business stakeholders to invest wisely, mitigate risk, become more efficient and make faster decisions

MITRE ATTACK FRAMEWORK

This is a globally-accessible knowledge base of **adversary tactics** and **techniques** based on real-world observations.

MITRE ATTACK FRAMEWORK

https://attack.mitre.org/

WHAT IS AN IOC AND IOA?

IOC Stands for Indicators of Compromise. Its an attribute (forensic data) associated with an attack.

- IOC focuses on **What** of an attack.
- Attributes attack to threat.

IOA stands for Indicators of Attack.

- IOAs focus more on the **WHY** and intent of an actor.

EXAMPLES OF IOC'S

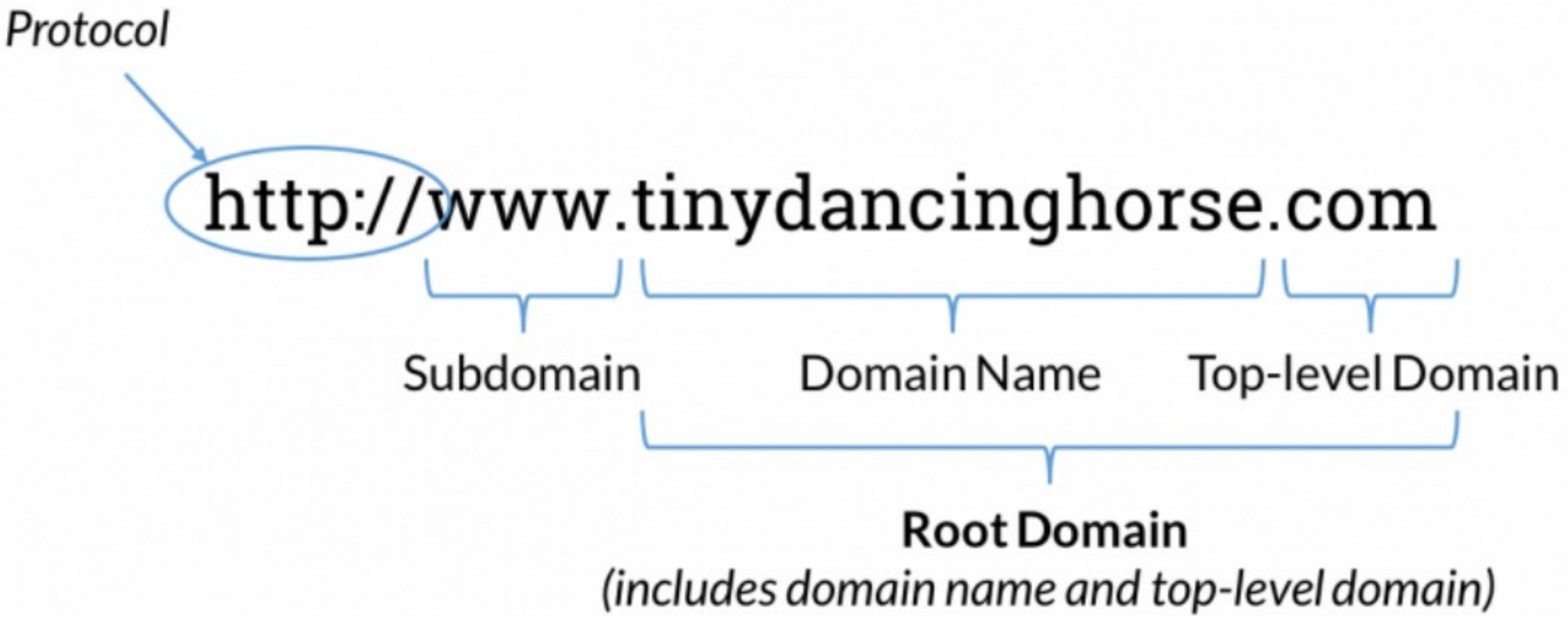
- IP addresses
- Domain names
- Emails
- Attachments
- URL's

DOMAINS

What is a domain?

A domain name, or domain, is the name of a website that you can type into your web browser to access it.

PARTS OF A DOMAIN



DOMAIN INFORMATION LOOK UP

https://whois.domaintools.com/

OSINT SOURCES

Websites and search engines
Social media
Public records
Forums and blogs
Government websites

METHODS FOR GATHERING OSINT DATA

Search engine queries
Social media monitoring
Data scraping
Public records request

USING OSINT IN CYBER SECURITY

Profiling potential attackers
Identifying phishing targets
Discovering vulnerable assets
Monitoring brand reputation

WHAT IS A HASH?

It’s a **fixed-length** string of characters randomly generated by an algorithm.

A hash ensures the **integrity** of a file is maintained (**NOT CHANGED**).

Why are hashes important

Data verification or data integrity

COMMON HASH ALGORITHMS

MD5 → **938c2cc0dcc05f2b68c4287040cfcf71** → **32 characters long**

SHA-1 → **2aae6c35c94fcfb415dbe95f408b9ce91ee846ed** → **40 characters**

SHA-256 → **dffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f** → **64 characters**

SHA-3 →
a69f73cca23a9ac5c8b567dc185a756e97c982164fe25859e0d1dcc1475c80a615b2123af1f5f94c11e3e9402c3ac558f500199d95b6d3e301758586281dcd26

and more.

EXAMPLE USING POWERSHELL

How to get the hash of a file from powershell:

1- open powershell and create a file by running the command:

notepad example.txt

2- add some content to the notepad file then save it.

3. run this command to generate a hash

Get-FileHash -Algorithm SHA256 -Path example.txt

4- make a change to the content of the file in notepad.

5- run step 3 again to generate the hash and compare the hashes

2023 OSINT TOOLS

✅1. Threat Intelligience 101 >> **https://lnkd.in/gfpd__xz**

✅2. URL, IP, domain, file hash (**virustotal**) >> **https://lnkd.in/gNqxtn4d**

✅3. **URL** Sandbox >> **https://urlscan.io/**

✅4. Cisco Reputation Check >> **https://lnkd.in/g7uWdC5q**

✅5. Diagnostic & lookup tools >> **https://mxtoolbox.com/**

✅6. Open Source IPS >> **https://www.snort.org/**

✅7. CyberChef >> **https://lnkd.in/gVjZywKu**

✅8. Browser Sandbox>> **https://lnkd.in/gjA-QqdX**

✅9. IBM Reputation Check >> **https://lnkd.in/gt8iyHE5**

✅10. IP Reputation Check >>**https://www.abuseipdb.com/**

✅11. **Sandboxing** >> **https://any.run/**

✅12. URL Category Finder >> **https://lnkd.in/g4qQGsHG**

WHAT IS URLSCAN ?

URLScan is a security tool and service designed to **scan** and **analyze** URLs (**Uniform Resource Locators**) for potential **threats** and **malicious** content. It's often used as part of a web security strategy to help identify and mitigate web-based security risks

URL SCAN

Scan the following URLs and review the results:

→ http://**oskarbit.com**/

→ http://**e-uyap.com.tr**/

GOOGLE HACKING

Google hacking, also known as Google dorking or Google-fu, is a technique used by individuals to find information on Google search engines that may not typically be easily accessible through conventional searches.

GOOGLE HACKING

1. **Finding Directory Listings:** To find directories that should not be publicly accessible: ``` intitle:index.of ```

2. **Locating Specific File Types:** To find specific file types, such as PDFs or spreadsheets: ``` filetype:pdf confidential ```

3. **Searching for Login Pages:** To find login pages of websites: ``` inurl:login ```

GOOGLE HACKING

4. **Identifying Vulnerable Webcams:** To find unprotected webcams: ``` inurl:/view/index.shtml ```

5. **Finding Open Web Proxies:** To locate open web proxies: ``` inurl:":8080" proxy ```

6. **Discovering Vulnerable Servers:** To identify servers running specific software with known vulnerabilities: ``` intitle:"Welcome to Windows 2000 Internet Services"

GOOGLE HACKING

7. **Searching for Sensitive Documents:** To find documents containing sensitive information: ``` intitle:"Confidential" filetype:doc ```

8. **Exploring Database Backends:** To locate websites that might be connected to databases: ``` inurl:search.php?id= ```

9. **Finding Exposed CCTV Cameras:** To find exposed CCTV cameras: ``` intitle:"Live View / - AXIS"