**TIPs** 

Tools

Describe the behavior and methods used by cyber adversaries to achieve their objectives, helping organizations understand, detect, and defend against threats.

Tools are software, scripts, or utilities used by attackers or defenders to perform specific actions, such as exploiting vulnerabilities, conducting reconnaissance, analyzing systems, or mitigating threats.

They are traces or evidence left behind on a network or host system as a result of cyber activities, such as logs, files, registry changes, network traffic patterns, or anomalous behavior, which can help in detecting and analyzing attacks.

human-readable address used to identify resources on the internet, such as websites, and is translated into an IP address by the Domain Name System (DNS).

It is is a unique numerical identifier assigned to devices connected to a network, enabling them to communicate with each other by identifying their location on the network

It is a fixed-length alphanumeric string generated by applying a cryptographic hash function to data, used to verify data integrity, identify files, or detect changes, as even small alterations to the input produce a completely different hash.

## artifacts Domain names

Network/host

IP addresses

Hash values