

HOW TO: NETWORK FOOTPRINT WITH MALTEGO

WHAT IS NETWORK FOOTPRINTING?

Also known as reconnaissance, footprinting is the technique used to gather information regarding a specific network environment. By performing network footprinting, analysts and investigators can get an overview of the infrastructure of a domain or website.

Network footprinting is usually used to reveal:



Vulnerabilities



Indicators of Compromise

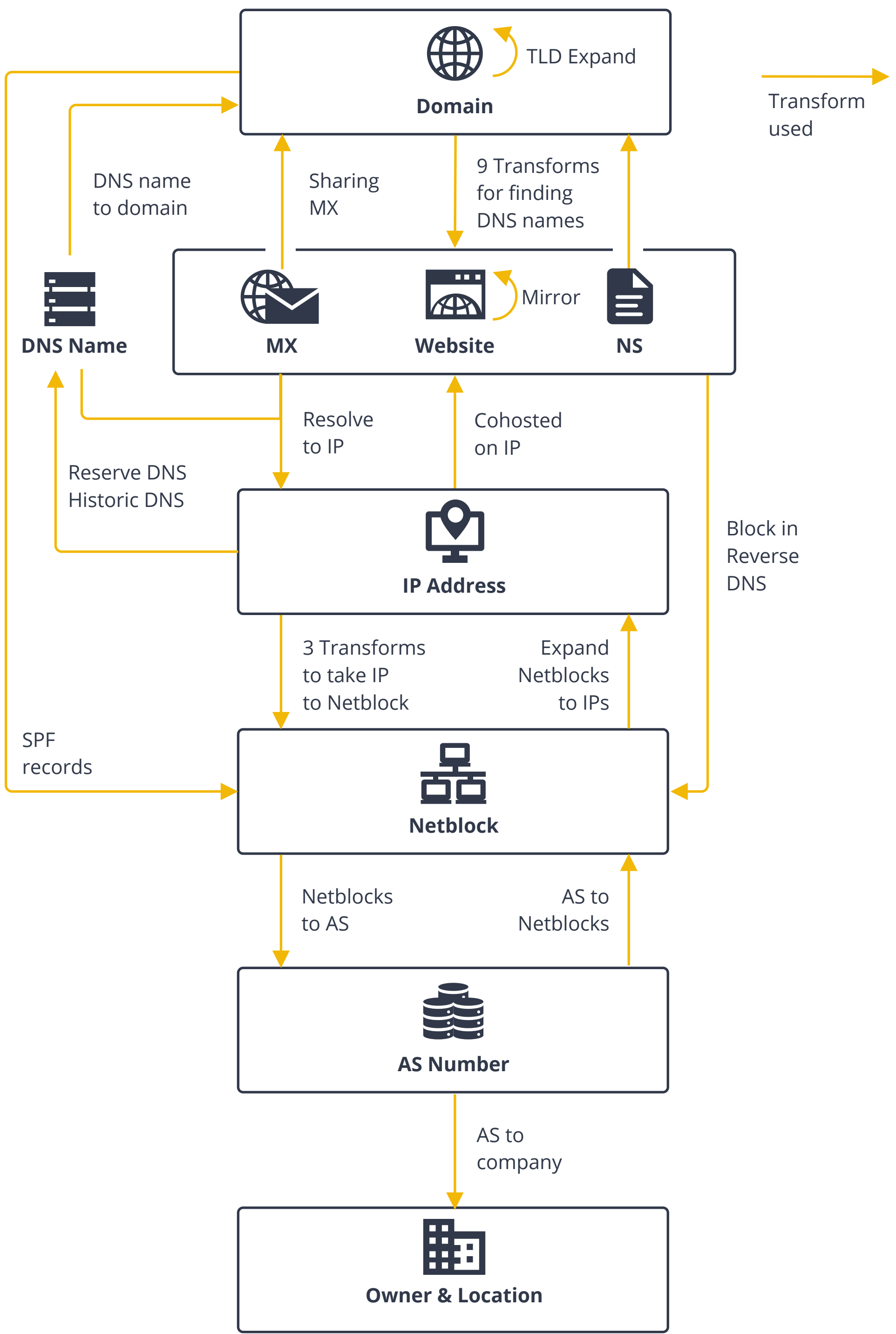


Hidden Weak Points

... and to improve current network policies and detection rules.

MALTEGO NETWORK FOOTPRINTING METHODOLOGY

Starting from a Domain Entity, Maltego users can perform a network footprint using several infrastructure Transforms. A network footprint can be created using the data model:



NETWORK FOOTPRINTING WITH MALTEGO: BEST PRACTICES

1

Follow the steps of the data model outlined here.

2

Ensure that the returned MX and NS are relevant to the target domain.

5

Follow the steps of the data model outlined here.

4

Ensure that the returned MX and NS are relevant to the target domain.

3

From IP Addresses, find historical DNS records via passive or reverse DNS lookup.

MALTEGO MACHINES: NETWORK FOOTPRINT AUTOMATION

Maltego Machines automate the process of running a sequence of Transforms. While users can create their own Machines, Maltego ships with three default Machines for network footprinting:

Footprint L1

Goes top to bottom of the data model to complete a basic footprint.

RESULT: BASIC

Footprint L2

Also looks for shared NS & MX infrastructures, websites hosted on the same IPs, etc.

RESULT: MODERATE

Footprint L3

Also looks for historical or reverse DNS data of netblocks and look for server technologies used by the websites.

RESULT: VERY COMPREHENSIVE

Speed up your network footprinting process and increase result precision with Maltego!

Want to discuss how your teams and organizations can conduct effective investigations with Maltego? Schedule a personalized demo today!

<https://www.maltego.com/schedule-a-demo/>

