NEST Kali Linux Tutorial: Maltego

“Maltego is an open source intelligence and forensics application. It will offer you timeous mining and gathering of information as well as the representation of this information in an easy to understand format.”

Catherine Zittlosen
November 2013

Maltego offers an aggregation of information posted all over the internet - whether it’s the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information.

Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego.
• Maltego allows you to enumerate network and domain information like:
  – Domain Names, Whois Information, DNS Names, Netblocks, IP Addresses, etc
• Maltego also allows you to:
  – Do simple verification of email addresses
  – Search blogs for tags and phrases
  – Identify incoming links for websites
  – Extract metadata from files from target domains
Introduction

- Maltego also allows you to enumerate People information like:
  - Email addresses associated with a person’s name
  - Web sites associated with a person’s name
  - Phone numbers associated with a person’s name
  - Social groups that are associated with a person’s name
  - Companies and organizations associated with a person’s name, etc
Open Maltego

- Applications > Kali Linux > Information gathering > DNS Analysis > Maltego
• Because we are using Maltego for the first time, we need to log in.
• Click “Next” at the prompt
Login

• Login with the credentials provided (during training session only).

• Click “Next”
• You will see a welcome message when you have successfully logged in.

• Click “Next”, “Next”, and then “Finish”
• You will begin to setup Maltego when you select transform seeds.

• Click “Next”
Update

- You need to update the transforms.
  
  ![Update wizard screenshot]

- Click “Finish”
Run

- Click “Cancel” on the last setup step.
- We will do it manually.
Domain Info

- Click on new icon for gathering the information
• Expand Infrastructure (on the left) and drag “Domain” into the “Main View”
Domain Info

- Double click on domain icon and rename it to “thinkgeek.com”
- Right click on domain icon and click 
  - Run Transform → All Transforms → To Website (Quick Lookup)
Domain Info

- We are going to find the IP address of our target website.
- Right click on the new icon that appeared
  - Run Transform → Resolve to IP → To IP Address (DNS)
Views

- You can change your view now. There are options Main View, Bubble View, and Entity List. You can explore these views for a different graphical representation.

- Also, note that there is a detail view and property view pane on the right with more information.
Email Addresses

- Right click on middle icon and then
  - Run Transform → All Transforms → Mirror: Email addresses found

- It may take a few minutes to populate the results
Email Addresses

• You can see the email addresses now
External Links

- Right click on target website icon and then
  - Run Transform > Links in and out of site > Mirror: External links found

- It may take a few minutes to populate the results
Clear Info

- You can drag and select the icons you want to remove.
- You can also type “CTRL-A” to select all and then click “Delete” on your keyboard to remove everything.
Facebook Profiles

• Expand ‘Personal’ in the left view
• Drag “Person” into the “Main View”
• Double click on the person icon and rename it to someone – eg. your name.
• Right click on target person and then
  – Run Transform > All Transforms > ToFacebookAffiliation
• Type “Yes” or “No” based on how many results you want.
  – “No” is more likely to find the correct result but will have many wrong hits as well
• Check “I accept the above disclaimer”
Lookup Email Addresses

• Right click on target person and then
  – Run Transform > All Transforms > To Email Address
    [Verify common]
• Right click again and then
  – Run Transform > All Transforms > To Email Address
    [using Search Engine]
• Type a space into both fields and click “Run!”
• You can play around with the other Options and test other things on the left Palette.
References