Maltego tutorial - Part 1: Information gathering

Karthik R, Contributor

Read the original story on SearchSecurity.in.

For effective and successful penetration testing, information gathering is a prime aspect, and must be given utmost importance by security researchers, according to the Open Web Application Security Project (OWASP). An attacker will attempt to gather as much information about the target as possible before executing an attack. This enables the attack to be more refined and efficient than if it were carried out without much information about the target.

This tutorial covers the usage of a very powerful open source intelligence (OSINT) tool known as Maltego. This tool has been mainly designed to harvest information on DNS and whois, and also offers options for search engine querying, SMTP queries, and so on.

Maltego offers broadly two types of reconnaissance options, namely, infrastructural and personal. Infrastructural reconnaissance deals with the domain, covering DNS information such as name servers, mail exchangers, zone transfer tables, DNS to IP mapping, and related information. Personal reconnaissance on the other hand includes personal information such as email addresses, phone numbers, social networking profiles, mutual friend connections, and so on.

Maltego framework and advantages

Maltego uses seed servers by sending client data in the XML format over a secure HTTPS connection. Once processed at the server side, the requested results are returned to the Maltego client.

Gathering of all publicly available information using search engines and manual techniques is cumbersome and time consuming. Maltego largely automates the information gathering process, thus saving a lot of time for the attacker, as we will see in this Maltego tutorial. The graphical display of information mined by the software aids the thinking process of the attacker in determining interconnected links between each entity.

A personal reconnaissance demo using Maltego

In this Maltego tutorial we shall take a look at carrying out personal reconnaissance. We can enumerate various kinds of information from the name provided to us. These include email addresses, URLs, social network profiles of a person and mutual connections between two people. This information can be effectively used in a social engineering attack to either pawn the victim or to gather even more information needed for the attack.

Suppose say the attacker obtains the name of a person, mining of data related to the name would start with targeting the person's email-ID. Maltego offers email-ID transforms using search engines. This is explained in the screenshot shown in Figure 1.

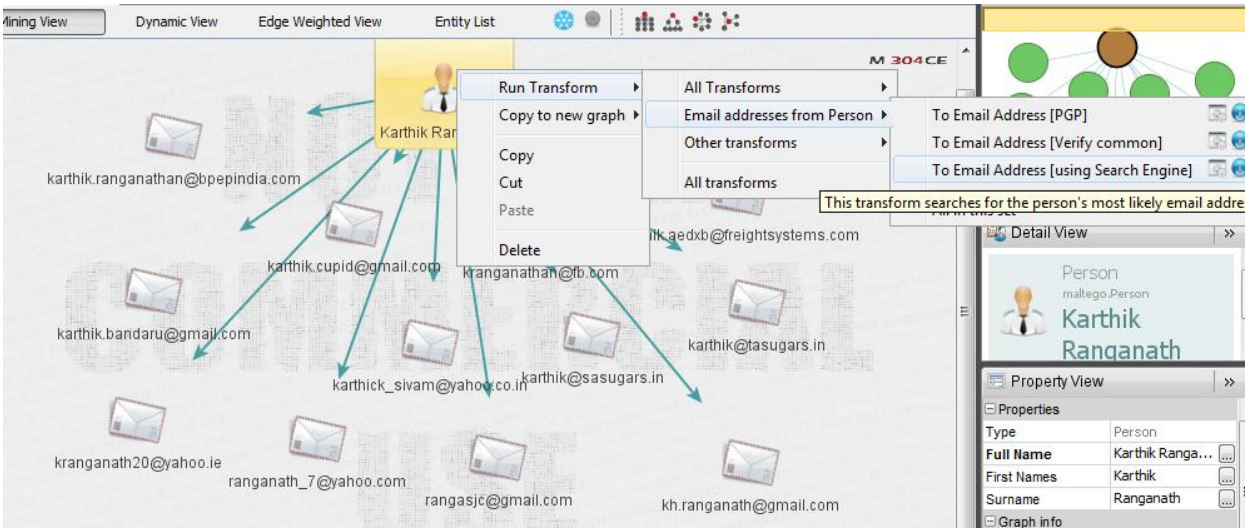

Figure 1. Data mining with Maltego

As is evident from Figure 1, the search engine query returns a large number of email addresses. For this Maltego tutorial we will use one email ID, and explain how to proceed further with the OSINT. In this example, running a transform "To Phone number" does not return any entity. However, running the transform "To URLs" unearths a silverstripe vulnerability, as shown in Figure 2. Let us keep this result aside for now.

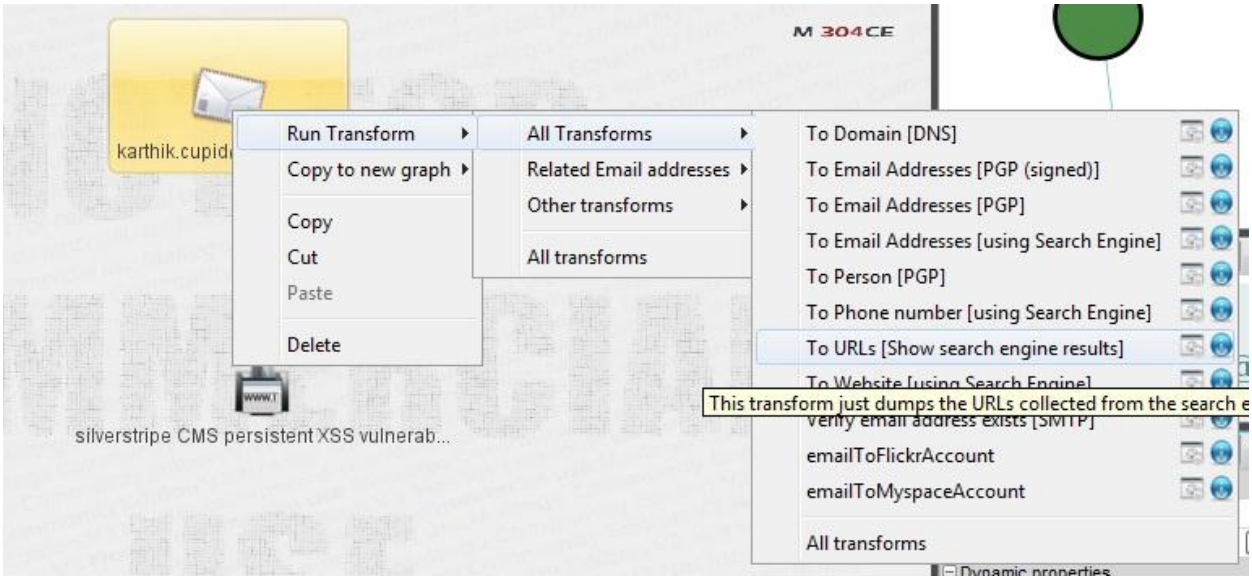

Figure 2. Transform To URLs reveals silverstripe vulnerability

Continuing this Maltego tutorial on personal reconnaissance, we will execute the "To Website" transform. This uses search engines to determine which websites the target email-ID is related to. The results are depicted in Figure 3.

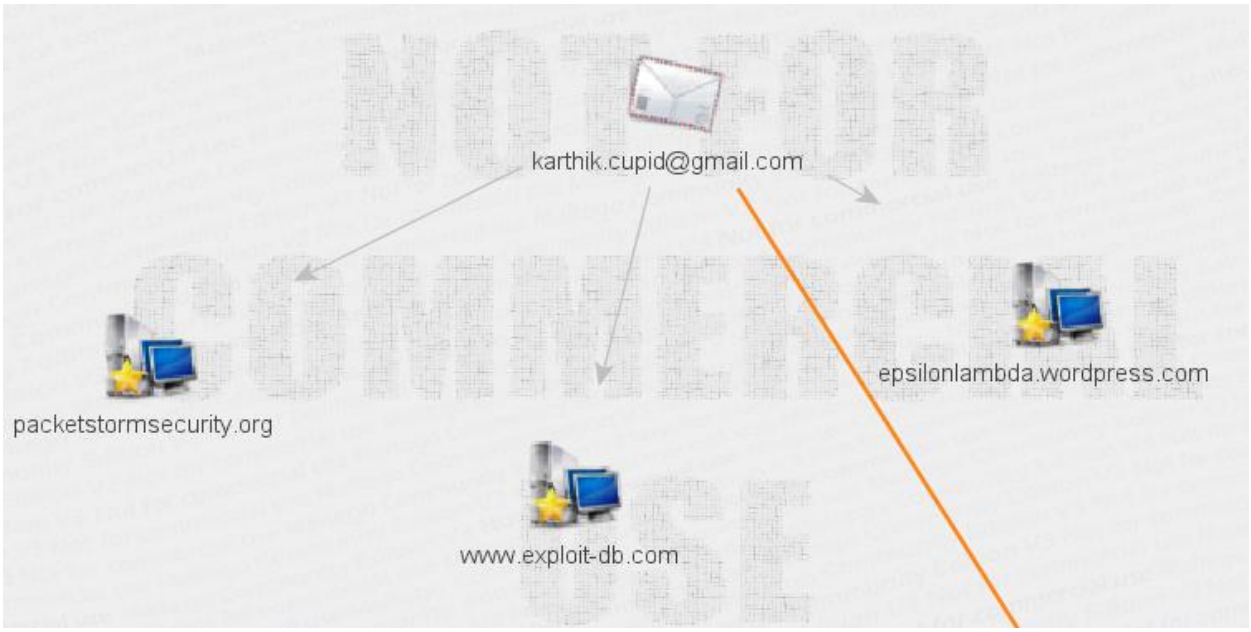

Figure 3. Websites associated with target email ID

From Figure 3 of this Maltego tutorial, we can clearly see that the target email-ID is associated with exploit-db, pss and a Wordpress blog. Interestingly, the blog belongs to the name we initially searched for, confirming our test to be accurate. In the next step of our Maltego tutorial we will run transforms over the silverstripe entity, as shown in Figure 4. We can see that it is further linked to the demo site, the email id, and also an association. This information is mined based on the "To Entities" transform, which uses natural language processing algorithms for data mining.

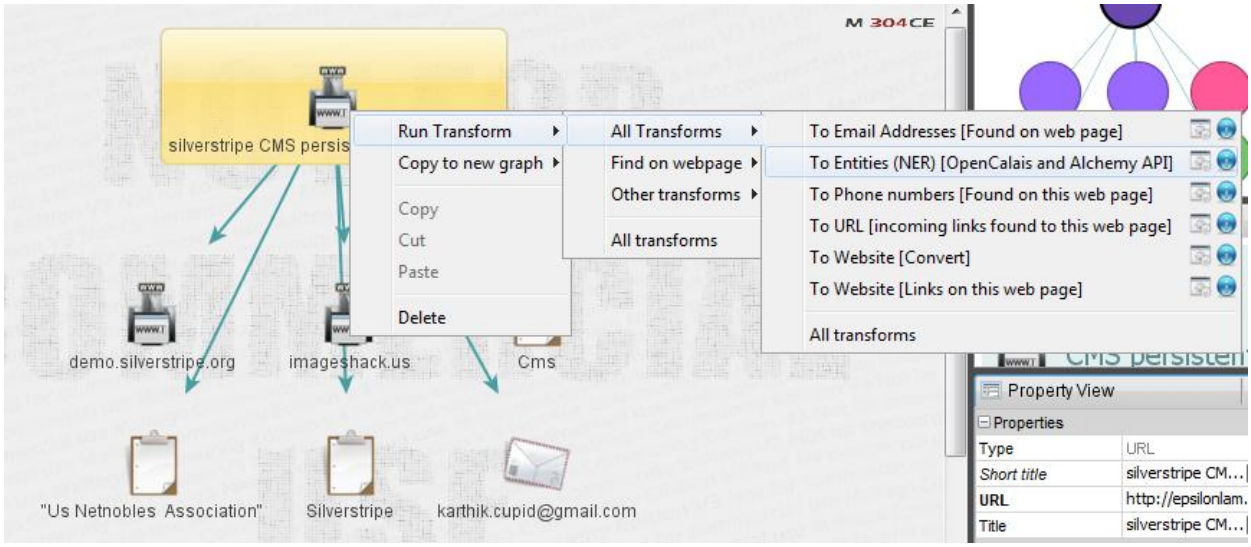

Figure 4. Transforms executed over the silverstripe entity

With Maltego it is also possible to find links into and out of any particular site. Maltego uses Gary Ruby's mirror to spider the target site and return the links that are related to it. This also returns the plugins used in a blog, links to social networking sites, Facebook pages, and so on.

Thus, we have taken a look at personal reconnaissance in detail in this Maltego tutorial. To summarize, starting out with just the name of a person, we obtained an email address on which we executed transforms, which in turn led us to an entity and a blog. We were able to establish external links with respect to the blog, and also determined the websites that the email ID was associated with. We were able to successfully determine the Facebook plugin used in the blog, which directly took us to the person's Facebook fan page.

Observing all the transforms in this Maltego tutorial, it can be concluded that Maltego indeed saves time on the reconnaissance aspect of penetration testing. To gather so much information using a search engine manually would be very tedious and would

require considerable mind mapping and visualization. Maltego provides us with a visual graphic illustration of each entity and reveals the relationships between them.

Instead of the name of a person, alternative starting points could have been a document, an email address, a phone number, a Facebook account, or something similar. Maltego provides a range of options within its personal reconnaissance section to run transforms. Of course, not all transforms would return results, so a measure of craftiness and quite a bit of patience would definitely be needed. The next installment of this Maltego tutorial will cover infrastructural reconnaissance using this amazing tool.

>>For more on Maltego, refer to tutorial no.2 in this series<<

About the author: ***Karthik R*** *is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at http://www.epsilonlambda.wordpress.com*

You can subscribe to our twitter feed at @SearchSecIN. Read the original story on SearchSecurity.in.

More Tutorials

- **Comprehensive tutorials for the infosec pro**
- **Metasploit tutorial part 1: Inside the Metasploit framework**
- **BackTrack 5 tutorial Part I: Information gathering and VA tools**
- **What is Wireshark?**
- **Burp Suite Guide: Part I – Basic tools**
- **Exploit writing tutorial: Part 1**