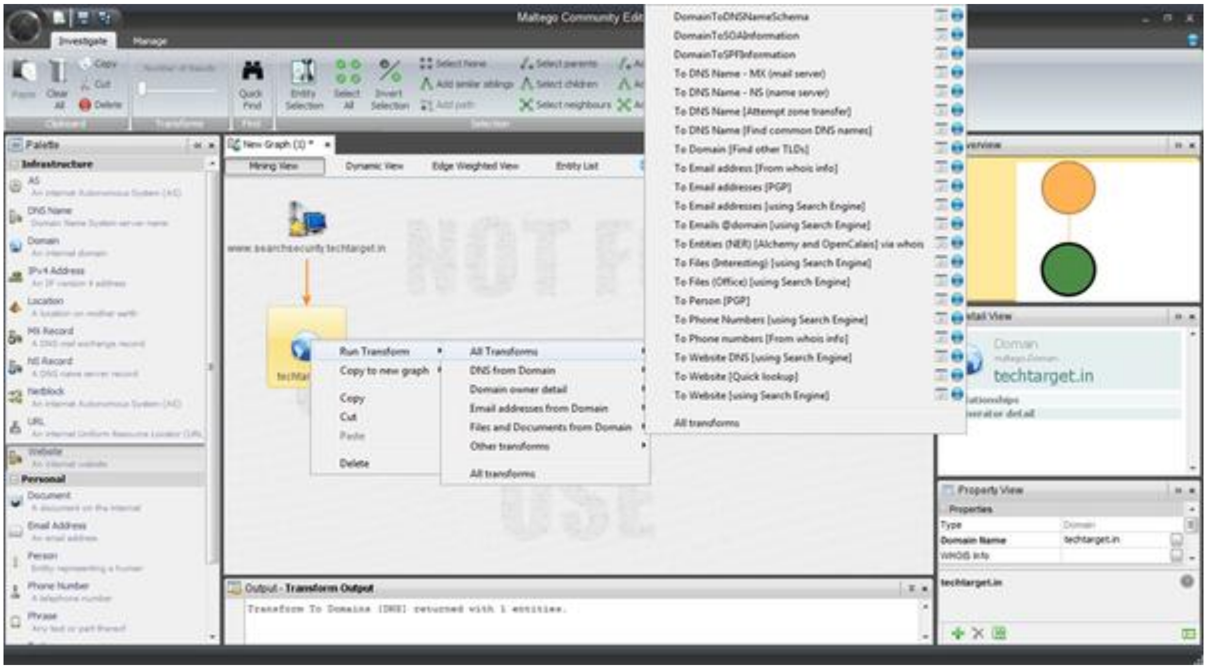
Maltego user guide part 2: Infrastructural reconnaissance

Karthik R, Contributor

Read the original story on SearchSecurity.in.

In the first installment of our Maltego tutorial you learned how to use Maltego for personal reconnaissance. Let us now discuss the infrastructural aspect of information gathering using Maltego. Infrastructural reconnaissance covers autonomous system (AS), DNS names, domain names, IPv4 addresses, mail exchange servers (MX), name servers (NS), and so on. From a reconnaissance point of view, it is important to enumerate the infrastructural details of the target. Here is a detailed demo of infrastructural reconnaissance using Maltego.


Maltego Community Edit
Investigate
Manage
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
URL
Website
Personal
Document
Email Address
Person
Phone Number
Phrase
New Graph (1)
Mining View
Dynamic View
Edge Weighted View
Entity List
www.searchsecurity.techtarget.in
techtar
Run Transform
Copy to new graph
Copy
Cut
Paste
Delete
All Transforms
DNS from Domain
Domain owner detail
Email addresses from Domain
Files and Documents from Domain
Other transforms
All transforms
DomainToDNSNameSchema
DomainToSOAInformation
DomainToSPFInformation
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To Domain [Find other TLDs]
To Email address [From whois info]
To Email addresses [PGP]
To Email addresses [using Search Engine]
To Emails @domain [using Search Engine]
To Entities (NER) [Alchemy and OpenCalais] via whois
To Files (Interesting) [using Search Engine]
To Files (Office) [using Search Engine]
To Person [PGP]
To Phone Numbers [using Search Engine]
To Phone numbers [From whois info]
To Website DNS [using Search Engine]
To Website [Quick lookup]
To Website [using Search Engine]
All transforms
Overview
Detail View
Domain
techtarget.in
Property View
Properties
Type
Domain
Domain Name
techtarget.in
WHOIS Info
Output - Transform Output

```
Transform To Domains [DNS] returned with 1 entities.
```

Figure 1. All transforms under infrastructural reconnaissance

Figure 1 clearly shows the range of available transforms. These transforms enable us to find the mail exchange servers, DNS names, persons associated with the organization, their phone numbers, emails on the domain, important files that are within the domain, and so on. Let us begin this Maltego guide explaining how to get information about MX servers.

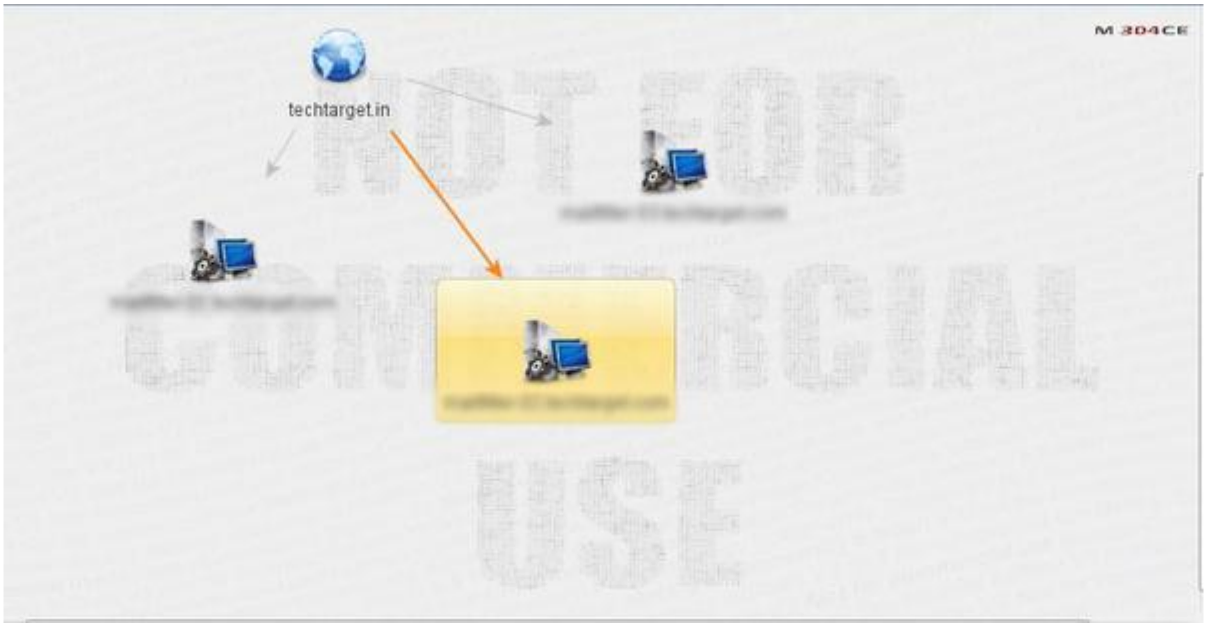


Figure 2. MX servers of a domain displayed in Maltego

Mail exchange servers can be a crucial element in an organization's security. Spammers connect directly to the MX servers to bypass security filters. Detecting the MX server is sometimes done by following common naming schemes. Generally, low priority MX records are used to target mail servers.

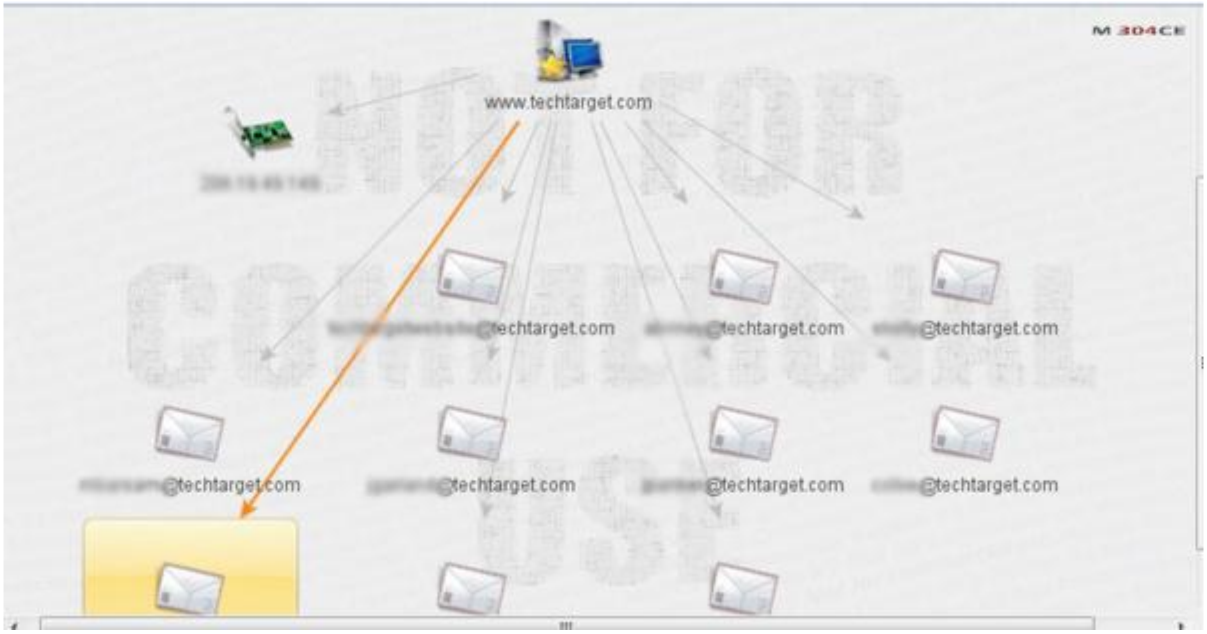


Figure 3. Gaining e-mail addresses of people from a site

As shown in Figure 3, we applied two transforms on the domain name. The first was to find the IP address and the second to find the email addresses. Establishing the IP address is very important, as this provides firsthand information of open ports, services and versions on the target. The official e-mail ids of an employee can be misused by sending him some crafted URL to inject malicious file in to his system, and harvest all details from the system and spreading the malware on the wire in the intranet.

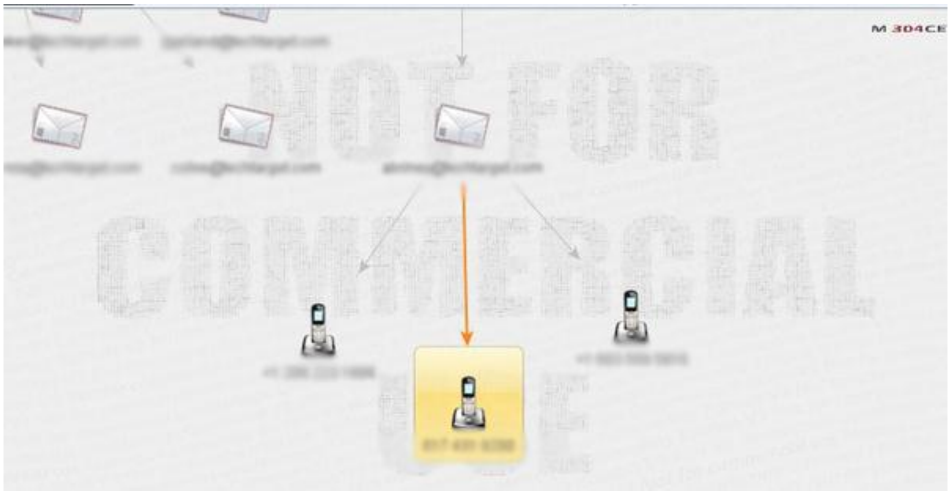


Figure 4. Harvesting phone numbers using Maltego

Using Maltego, a transformation to find out the phone numbers of user@website.com reveals three different numbers, as depicted in Figure 4. An attacker can use this information to perform tried and tested social engineering attacks on the concerned person, and possibly harvest additional information.

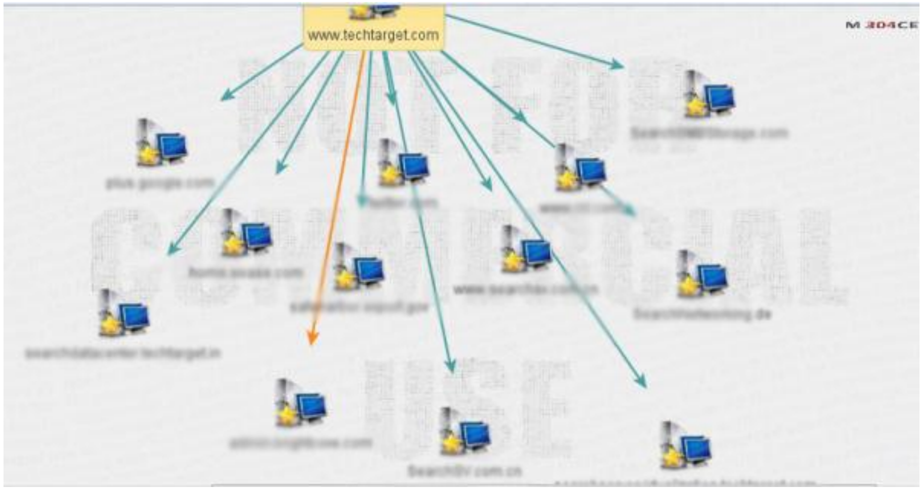


Figure 5. External links from Techtarget.com

For this Maltego tutorial we have determined the external links from the domain space of techtarget.com. As seen in Figure 5, there are several dependent or linked domains to the TechTarget domain space. These include some of the specialized units of the organization, few governmental agencies and other social media sites.

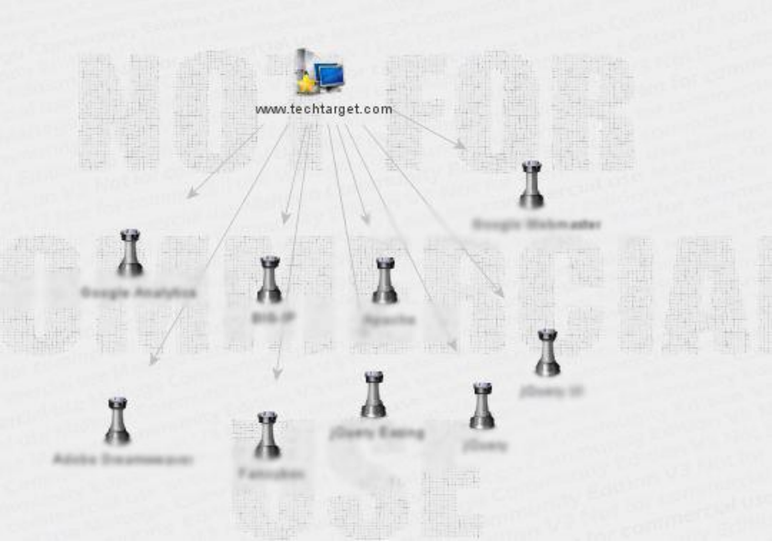


Figure 6. Determining server technologies of the target

The next transform using Maltego is to determine the server technologies used by the target application. As shown in Figure 6, the target uses services from multiple sources. Since we have zeroed in on the technologies used, this narrows down our search criteria when it comes to vulnerability research.

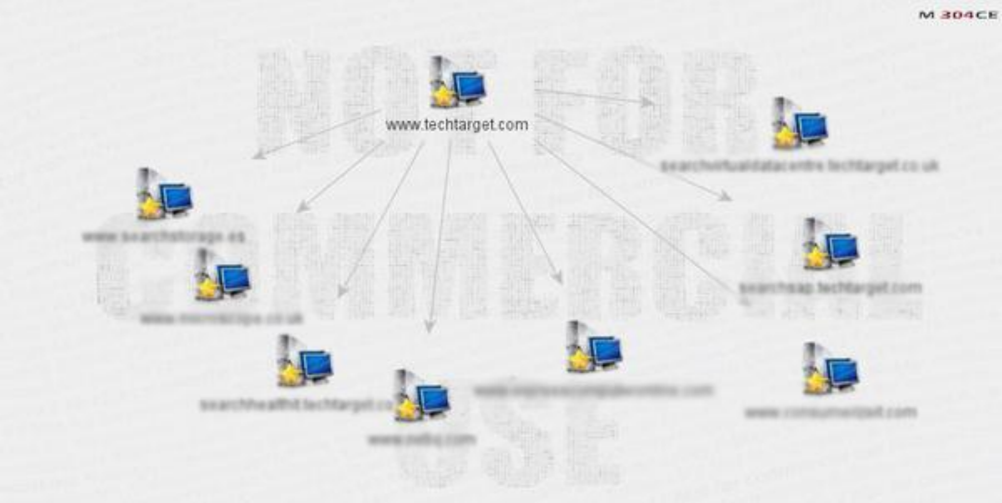


Figure 7. Incoming links to the site

With Maltego, another set of transformations can be used on the target to ascertain incoming connections to the target. Figure 7 reveals that there are a lot of units connecting back to the servers of techtarget.com.

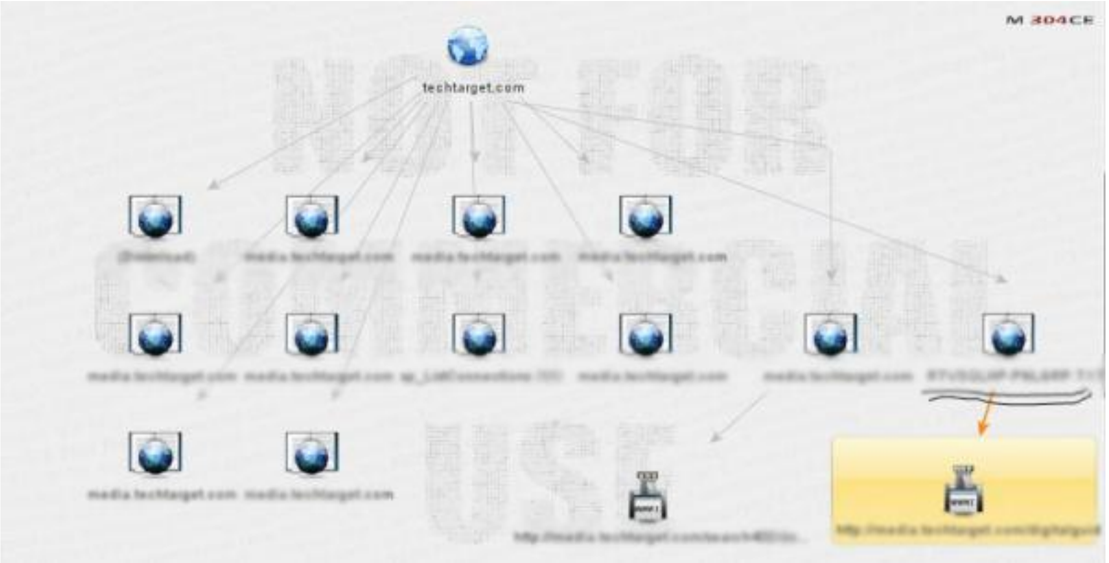


Figure 8. File transformations

In the next step of this guide to Maltego we will use the “To Files (Interesting)” transform in order to look for interesting files on the domain, and then find the meta data of those files. Unfortunately, this is not available. But, we could extract the URLs as seen in the last row to the bottom-right of Figure 8.

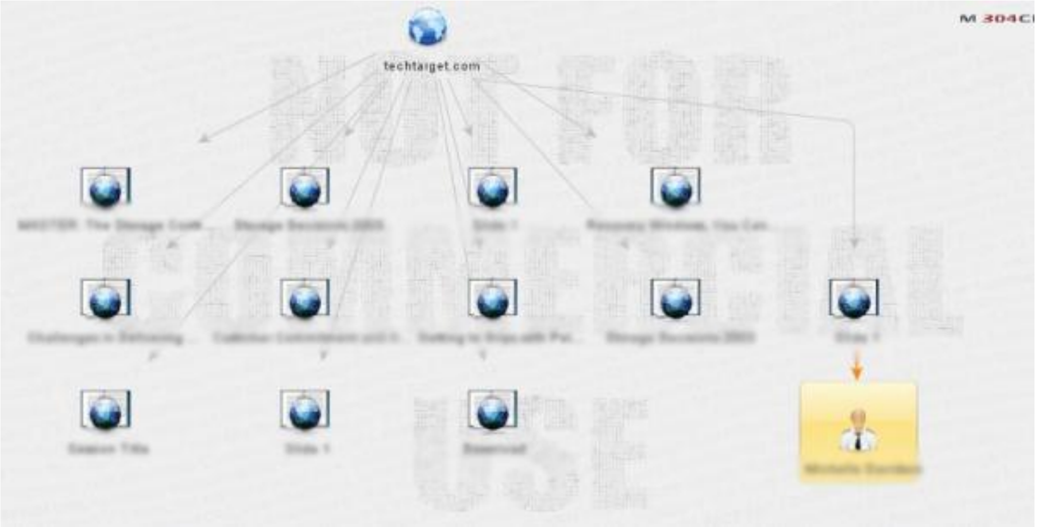


Figure 9. Official file transform and parsing meta data

Running the Maltego transform "To Files (Office)" reveals several entities, as seen in Figure 9. Personal reconnaissance on this entity could result in gathering a huge amount of information.

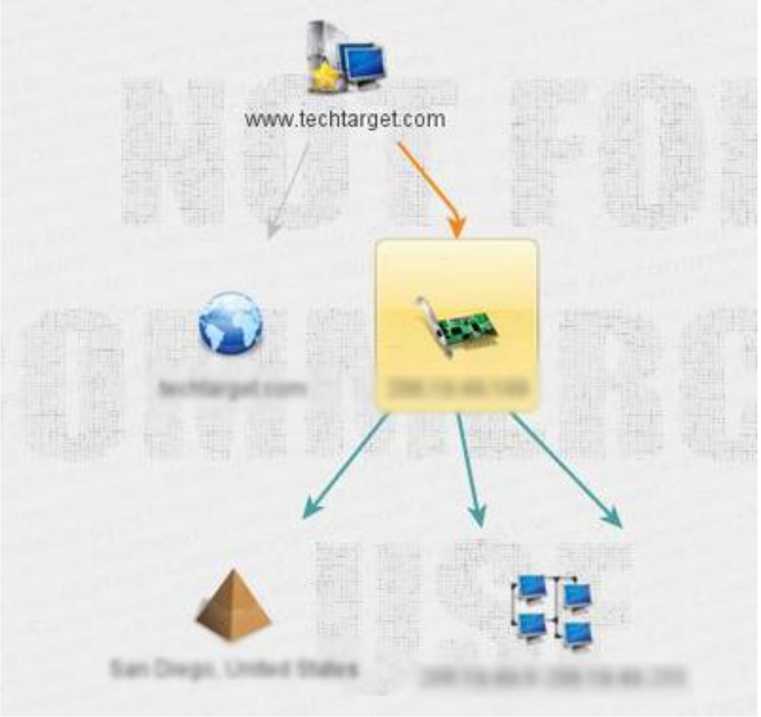


Figure 10. Finding geo location and NetBlock information

The last part of this Maltego tutorial covers aspects of social engineering and understanding the scenario of the attack. As we have seen, the first step is to apply transforms to obtain IP information. From the IP information we get the location on the globe. Following this, we can use Maltego to find the NetBlock information of the IP addresses.

This Maltego tutorial series has demonstrated most of the important transforms available, covering both personal reconnaissance and infrastructure reconnaissance. Clubbing the two, one can extract maximum data from the target. This would lead to effective vulnerability assessment prior to an attack. As explained earlier, optimal usage of tools such as Maltego depends purely on the creativity of the attacker. There is no limit to the information that one can extract. As we have seen in this Maltego tutorial, not all transformations work all the time. Using the right transforms on right entities will make your reconnaissance with Maltego a success story.

>>Read the first tutorial on information gathering with Maltego here<<

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**