

## Maltego Part II - Infrastructure Enumeration

By Chris Gates, CISSP, GCIH, C|EH, CPTS

Welcome Back! In Maltego Part I we performed Personal Reconnaissance with Maltego to see what we could find out on the net about our Editor-in-Chief, Don. With the personal details tucked safely away in our notebook, lets see what we can gather in regards to his network infrastructure.

Any organization that has an Internet presence needs to have some form of infrastructure to support their presence. During Infrastructure Enumeration you attempt to discover how much of it exists, what type of infrastructure is used, where it is located, what technology is used and how it is structured. This type of information is interesting for:

- \* Security assessments (as this is the first and most tedious phase of any external assessment).
- \* Getting an idea of the organization's Internet and geographical presence.
- \* Gaining insight into the technology used by the organization.
- \* Making connections between seemingly unconnected organizations (as they might be sharing common infrastructure).
- \* Getting a list of brands or affiliations supported by the organization.

Be sure to catch Chris at ChicagoCon 2009s on May 9 as he presents Attacking Layer 8: Client Side Penetration Testing with Vince Marvelli (g0ne). Get Conference Details [HERE!](#)

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Gates}

Chris Gates is a Scheduled Speaker for the Spring ChicagoCon

The Ethical Hacking Conference is May 8 - 9, 2009

## Infrastructure Footprinting

Infrastructure Footprinting is essential for identifying possible systems for remote attacks. An organization's full IP assets will normally not be readily available or determinable to a penetration tester. Therefore we have to use a combination of tools, creativity, brute forcing and luck to try to identify all the different infrastructure assets the organization owns. A good pen tester must also attempt to identify any trust or partner relationships the client may have as those partners may also be in scope for our assessment.

We'll primarily be working off of the Infrastructure Palette for infrastructure information gathering (makes sense right). Our personal reconnaissance of Don was primarily off of the Personal Palette.

## Figure 1: Infrastructure Palette

Each of your options are called entities and are explained here: <http://ctas.paterva.com/view/Category:Entities>

In general we start our information gathering with an organization's web presence. So we start with [www.digitalconstructionco.com](http://www.digitalconstructionco.com) using the DNS Name entity.

Use the `DNSNameToDomain_DNS` transform (for a full list of possible transforms go here: <http://www.paterva.com/maltego/maltego-server/modules/ctas-module/>) to get us down to a domain name.

Figure 2: Results of the DNSNameToDomain\_DNS transform

From there we can use the DomainToMXrecord\_DNS and DomainToNSrecord\_DNS transforms to locate the name and mail servers.

Figure 3: Results of the DNSNameToMXrecord\_DNS transform

Then use the DomainToDNSName\_DNSBrute transform to find as many possible domain names for digitalconstructionco.com domain. This transform does a dictionary brute force lookup of possible domains. You can add words to the transform by going to Tools --> Manage Transforms

Figure 4: Manage Transforms Options

Click on the Display Name to sort the transforms and click on the To DNS Name [Brute] transform.

Figure 5: Selecting To DNS Name [Brute] transform

In the Transform inputs -->Optional inputs--> field (lower right) you can add additional domain name prefixes to test.

Digitalconstructionco.com didn't yield much in the way of additional domain names. Only www (which we already knew) and ftp.

Figure 6: Results of the DomainToDNSName\_DNSBrute transform for digitalconstructionco.com

Microsoft.com yields several more and shows a bit more of the power of Maltego to manage large networks.

Figure 7: Results of the DomainToDNSName\_DNSBrute transform for microsoft.com

Next we take our domain names, NS, and MX servers to IP addresses using the DNSNameToIPAddress\_DNS transform.

Figure 8: Results of the DNSNameToIPAddress\_DNS transform

While this transform might not seem like much from our digitalconstructionco.com example, it can be handy to quickly determine that an IP address has multiple DNS names point to it. For example, in the Microsoft domain we were able to quickly and visually see that seemingly unrelated DNS names resolve to the same IPs.

Figure 9: Results of the DNSNameToIPAddress\_DNS transform for parts of asia.microsoft.com

Two IP's of asia.microsoft.com with tons of other DNS nams resolving to those IPs as well.

Figure 10: Results of the DNSNameToIPAddress\_DNS transform for parts of asia.microsoft.com

You can also select an IP address and look at the Detail View to see the domain names that resolve to it.

Figure 11: Detail View for parts of asia.microsoft.com

To quickly and visually see the above, after you've resolved those DNS names to IPs you might want to show the 'Edge weighted view', which will quickly show which IP addresses are central to their organization. For more information on the views, check out the Maltego Wiki.

Figure 12: Edge Weighted View for our Microsoft IPs showing that many hosts point to two IPs

To get a quick list of (some of) their domains QUICKLY - get the NS for microsoft.com - then run NSrecordToDomain\_SharedNS. It will find all the domains that share that NS. Your results versus accuracy slider will be

important for this transform. Obviously the more you slide toward #of results the more results that will be returned which can be substantial depending on the nameserver.

Figure 13: Results of the NSrecordToDomain\_SharedNS transform with results bar on the accuracy side.

Figure 14: Results of the NSrecordToDomain\_SharedNS transform with the results bar on the results side.

We can also do a DNSNameToDomain\_SharedMX transform that will show us other domains that use the same MX records, thus finding other domains that may be in scope.

Figure 15: Results of the DNSNameToDomain\_SharedMX transform on microsoft.com public facing mail server

Next up is to take each of those IP addresses and turn those into netblocks using one of the following transforms; IPAddressToNetblock SS (SS = ServerSniff), IPAddressToNetblock NS4block, IPAddressToNetblock Cuts.

Figure 16: Results of the IPAddressToNetblock\_SS transform

Of particular usefulness is the IPAddressToNetblock Cuts transform that allows us to break a large netblock into manageable pieces. This is important because the NetblockToDNSName SS and NetblockToDNSName RevDNS transforms only allow max 2048 lookups at a time, I normally break it up into a 256 host chunk (which is the default). This is a manageable chunk unless you are sure the domain you are looking at actually owns the full net block and you need to find all the DNS names the bruteforce transform missed. Let's see the IPAddressToNetblock Cuts transform within the Tools--> Manage Transforms menu. We could change the block size in the optional inputs section.

Figure 17: Manage transform options for To Netblock [cuts] transform

and the IPAddressToNetblock Cuts transform output:

Figure 18: Output of the IPAddressToNetblock Cuts transform. We can also see the output of the NetblockToAS and NetblockToLocation transforms.

A way to QUICKLY get an organization's netblock(s) - get the NS records for microsoft.com, select all and run

NSrecordToNetblock\_NS4block. That transform will look on Robtex to see which netblocks those nameservers are delegated to. You very quickly have a list of netblocks to take a further look at.

Figure 19: Results of the NSrecordToNetblock\_NS4block transform on one of microsoft.com's nameservers.

We can also reverse lookup any of the netblocks 2048 hosts or less

Figure 20: Results of the NetblockToDNSName RevDNS transform.

## Wrap Up

So in conclusion, we took a "black-box" approach starting just with a domain name and showed the various ways we can determine:

- \* Domains and possibly shared and partner domains.
- \* DNS names via reverse look-ups and brute force.
- \* IP Addresses for domain names and important servers.
- \* Networks and Netblocks used or owned.

Also possible but not shown was:

- \* Physical distribution of infrastructure by using the IPAddressToLocation\_WhoisAPI transform.

Huge thanks to Roelof Temmingh of Paterva for all the help with both articles!

## Extra Resources

Maltego Wiki: Educational Videos

<http://www.paterva.com/maltego/screenshots/>

#2 is extremely good in showing you how the visual representations make it easy to see the linkage between the two

sites.

Check out the Maltego Forum

<http://www.paterva.com/forum/>

Mubix, over on the room362 blog has been doing a series of articles on Maltego.

<http://www.room362.com/archives/186-maltego-2-and-beyond-part-1.html>

<http://www.room362.com/archives/190-maltego-2-and-beyond-part-2.html>

<http://www.room362.com/archives/225-maltego-2-and-beyond-part-3.html>

Using NLP for Information Gathering

<http://blogs.technet.com/bluehat/archive/2008/09/22/using-nlp-for-information-gathering.aspx>