# 1. METHODOLOGY – FORMS

Collecting information during a penetration test is a scientific process that prepares and gives you better chances at reaching your goal: finding, exploiting and reporting all of the vulnerabilities in the target systems.

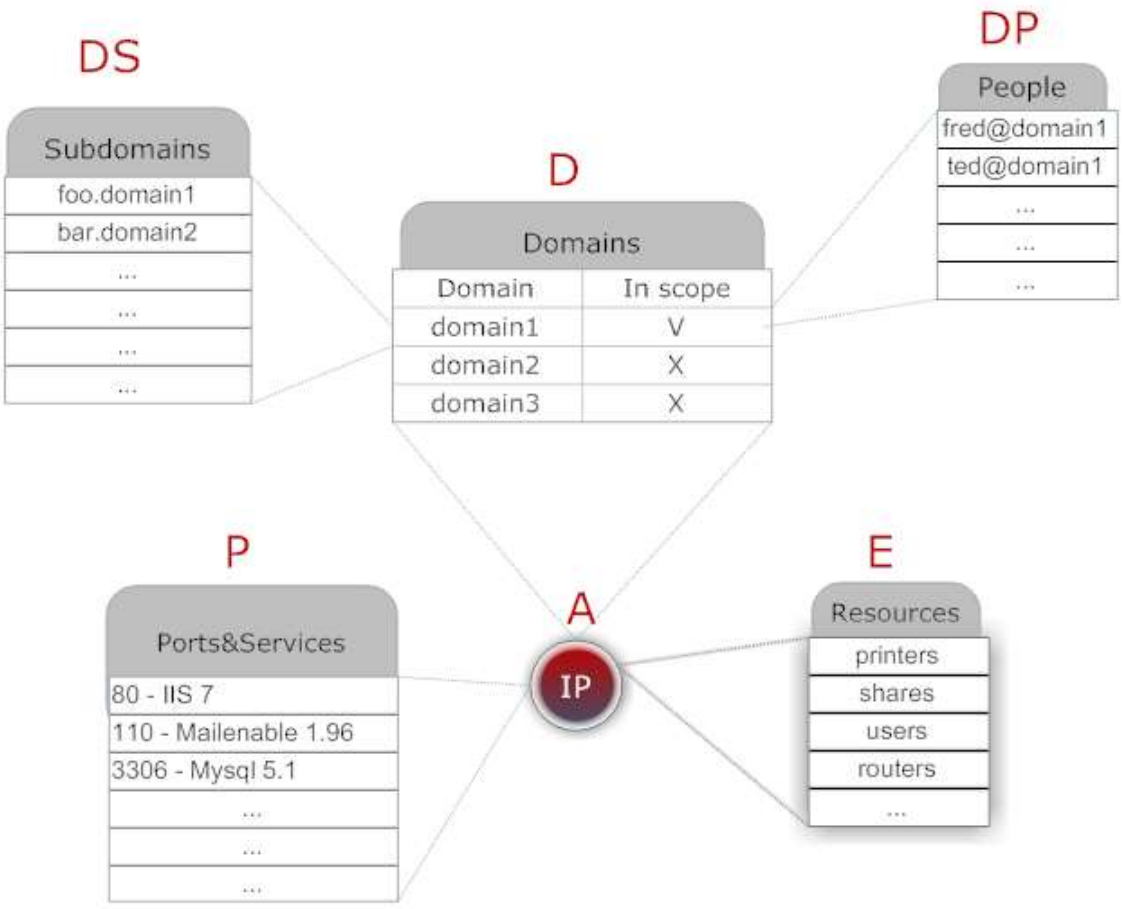
The following is the proposed Information collection methodology scheme.
With the intent of improving the way information is collected during a penetration test, you will find a number of forms.

These forms will help you keep your engagement files (and information) organized in every phase: from information gathering to preparation for exploitation.

Every form is indicated with a letter for reference within this document and the forms: you will find that these forms are related to each other similarly to how relational databases link tables together.

This methodology should not be considered as the best possible.
The most organized and experienced penetration tester already has a time-tested information collection methodology built around his habits and attitudes at personal work organization.
This methodology, although covering 90% of the information you may need to collect during a penetration test, can be improved and (we strongly advise it) customized according to: type of engagement, your attitude at arranging information and your liking.
Forcing you to follow our own strict methodology would decrease the chances of success in reaching our final goal: inviting you to follow a scientific approach while handling your penetration testing information.

# 2. MAPs


DS
Subdomains
foo.domain1
bar.domain2
...
...
...
...
D
Domains
Domain
In scope
domain1
V
domain2
X
domain3
X
DP
People
fred@domain1
ted@domain1
...
...
...
P
Ports&Services
80 - IIS 7
110 - Mailenable 1.96
3306 - Mysql 5.1
...
...
...
A
IP
E
Resources
printers
shares
users
routers
...

# 3. FORMS

A This form contains the IP addresses in the scope of your engagement. Here you will collect information such as, geographical location, net block number and owner.

D This form contains all the domains found on a given IP. This table is related to A through the A column. Not all the domains (usually all or none) will be in the scope of your engagement. You will make sure to mark with a visible V the ones that are, and with a X the ones that are not.
Note that the webserver is present both here and the DS form in case domain.com webserver is different from www.domain.com

DS Subdomains and the related information will be stored here. If web application security is in the scope of engagement you will want to insert even more details in this table. However a link to W forms is given. These forms are specifically designed for web application security testing engagements.
Note that this form is related to D since a domain can have multiple subdomains.

DP DP form contains information about people: emails, addresses, accounts into forums and social networks and so on. This form will be specifically useful for Social Engineering attacks. Sometimes emails are related to departments instead of single persons and sometimes you will be even able to understand the position of the person from the documents metadata produced or the Headers of email addresses.

P This form will be filled after you have used your favorite port scanning tool, namely nmap. If you're able to gather the banner or the version of the service you will have this form almost ready for mapping the attack surface stage.

E This form stores the results of the Enumeration phase.
Netbios Shares, printers, usernames, password policies and so on.
Since this information is very heterogeneous you will need to further classify it through the column Type. Possible values can be "shares", "usernames" etc.

# 4. MAPS

Alternatively or in conjunction with the above method, you can use mindmapping to visually organize information while pentesting.

In this chapter we will see some basic rules to achieve an effective information storage process through the open source and multi-platform mind mapping tool FreeMind.

Teaching how mindmaps work is beyond the scope of this document.
We want to exploit the features of a mindmap for our purposes: storing and visually organize data during a penetration test.

Using FreeMind will let us:

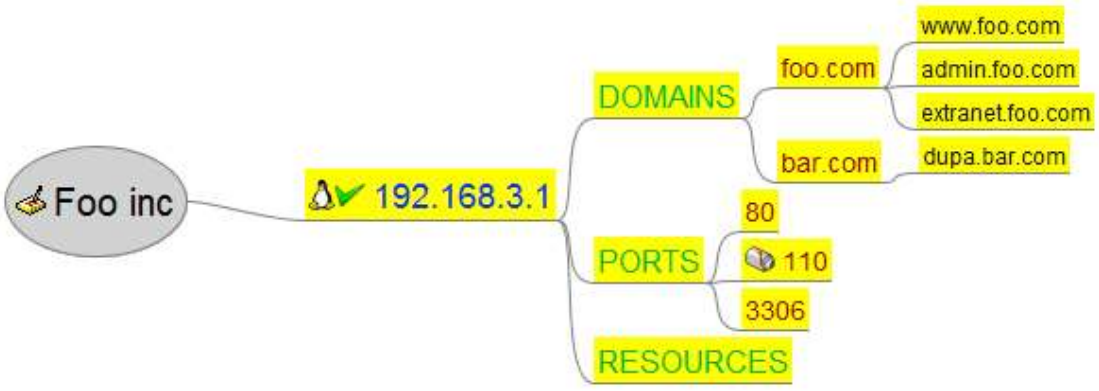
- Easily create graphical hierarchies
- Add comments to each node
- Add icons to each node
- Link nodes together according to some relationship patterns
- Export the map to PDF or Image to be included in our final report

This document wants to provide the basic rules to categorize penetration testing data through mindmaps.

More advanced rules can be created according to the scope of engagement.

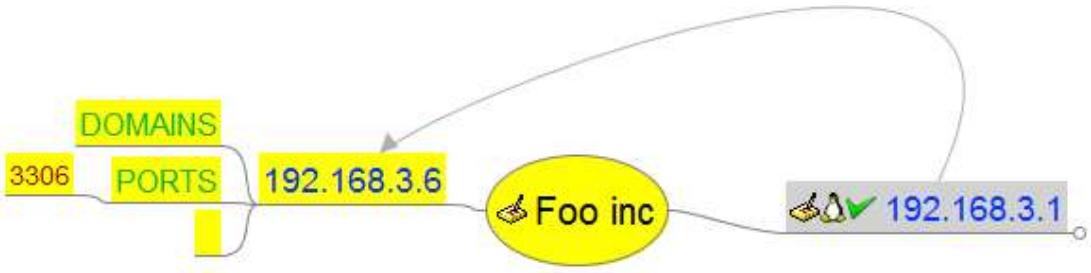
The general categorization of our mindmap will be:


- Main topic will be our engagement (usually it coincides with the client company or it can be a part of it e.g.: “First phase Foo inc.”)
- Second level, for a network penetration test, will be the IP addresses in scope. If IP addresses are not given and discovery is part of the engagement you will add new IP’s in your discovery process. If IP’s are given you will pre-populate them in your map.
- Third level holds all of the aspects belonging to second level, IP addresses. A minimum set is PORTS, RESOURCES. If web domains are presents you will add this level too.
- Fourth level can finally contain the actual data gathered during the first phases of your penetration test.



## 4.1 RELATIONSHIPS

Building hierarchical information is easy and lets us keep track of information in a very handy manner. You are able to expand/collapse and link together different branches of the tree:




With the arrow we can visually spot a link between two IP's.
In the above image 192.168.3.1 is hosting multiple domains (now folded so invisible) which use a Mysql server on 192.168.3.6.

You add a link between two nodes by selecting them, right click and choose Insert->Add Graphical Link

The importance of immediately spotting relationships and connections between two targets will be highly appreciated while working out an exploitation plan.

## 4.2 CONVENTIONS

We can get a little more visual help by using Icons. We can associate icons to every node of our map. This is especially useful for IP's: You can associate icons of Linux or Windows or Solaris etc. according to the results of your OS fingerprinting phase.

Moreover it would be extremely helpful for your penetration testing process and your own productivity to choose 3 icons to associate to the following status:

- Tested
- In process
- To test


In case you do not perform the penetration testing work alone, but instead you work in a team, you may want to agree the use of these icons with your colleagues and maybe use different icons to assign the tasks (the analysis of each node) to different colleagues.

The information gathered in a penetration testing task grows exponentially.
The use of hierarchical representation (with possibility of interconnecting nodes in a network) and icons can save you a lot of time.

If you want to add more icons to the default ones follow this trick:

1. Open the `freemind.jar` with Winrar or any other similar tool.
2. Extract it
3. Find the folder `\images\icons` and add your new icons there
4. Re-package the whole folder again (you will create a .rar file that will have to be renamed again into a freemind.jar)

## 4.3 FILES

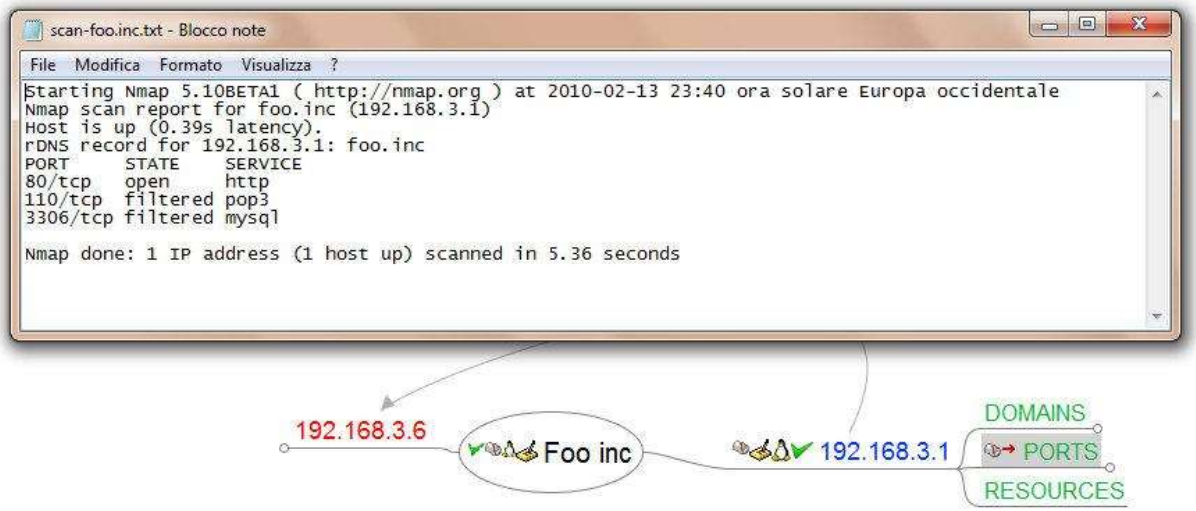
The Forms and the Mindmap are two different ways of storing information.

However the two can easily be combined together by means of the Hyperlink to file supported by FreeMind.

Right click on a node, Insert->Hyperlink (File chooser)

You will be able to link a file to a node. This file will be opened everytime we will click on the little arrow appearing beside the node name.

This is extremely useful when we don't want to add too much information to the map (for different reasons) or when we want to use the best from the two approaches: the verbosity of the Form based approach and the beauty of having everything at a glance:




The above image pictures a common scenario in which you may want to link the output of Nmap to your PORTS node.

# 5. CONCLUSIONS

By now you should be convinced of the importance of using a well defined methodology while pentesting. The success of the penetration test relies on your attitude and precision much more than on the tools you use to actually perform it.

While complying with a tight methodology may be too restrictive and not always the case, creating your own information organization schema is something you should do and improve with time.

You will find yourself polishing your methodology files and tool-set at every new engagement.

This document surveyed the two possible approaches that according to our direct experience in the field produce the best results in terms of productivity and efficiency.

You can follow one of the two approaches, or the two combined together, and move on from customizing it according to your environment, needs and liking.

Version 1 – 14/04/2010