Practical Attack & Defence
Kimmo Saurén
Metropolia

Exercise 1. Information gathering and reconnaissance

The Internet is full of organisations and companies. All of them reveal information about themself intentionally and unintentionally. For criminals this information is valuable for gaining unauthorizated access to computer systems.

Internet criminals have few general strategies to gain access to valuable information.

- Attacking a specific company / network
  - This requires more skillfull hacking because one has to find weak points in the computer system under attack. Reconnaissance activities play a major role in this type of attack since attacker wants to avoid detection as much as possible.
  - Usually in this case attackers are aware what they want from the target company or network.
- Attacking any weak computer system or network in the Internet
  - In this methods attackers are taking an opportunistic view of hacking. Using reconnaissance techniques attackers try to locate weak points and eploit them.
  - Attackers are not usually aware what they will gain from system. They might steal sensitive information or they just might use the compromised system for hiding further illigal activities,
  - In this method attackers might consentrate for certain vulnerabilities or use Google to find open systems.

In this exercise we are making reconnaissance activities against metropolia's network.

Reconnaissance can be divided into two different categories:

1. Silent reconnaissance
   In this recon type attacker will not make any unnatural connection attempts to the target system. Usually this activities are not considered illegal by any country. Attacker can for example:
   - find out IP-ranges using whois queries
   - use domain name servers to find out corresponding names for IP-addresses
   - use Google hacking for retrieve useful information
   - use Google cache for retrieving cached web-pages of the target system
   - find out people, phone numbers, anddresses and so on about the target system for social engineering

2. Unsilent reconnaissance
   In this recon type attacker will take more direct approach. He will make queries to the target network. This phase is naturally followed after silent recon. It is also more accurate because of silent recon performed earlier. Of course the attacke still tries to be as silent as possible, but he knows that these activities can be noticed. These activities are considered to be illegal.

   In unsilent recon attacker can for example:

- perform IP-address scan to find out alive systems in network
- perform port scans to find open services
- perform scans to map firewall rule sets
- browse webpages of the organization to find weak points
- download the whole webpage for offline inspection

These are some steps that attacker can take to make successful recon on the target organization. Reconnaissance is however considered an art as much as skill. And because of that exact step that are part of recon activites depend on the system under study.

Social engineering is also very important part of these activities and usually the most effective way to get into systems.

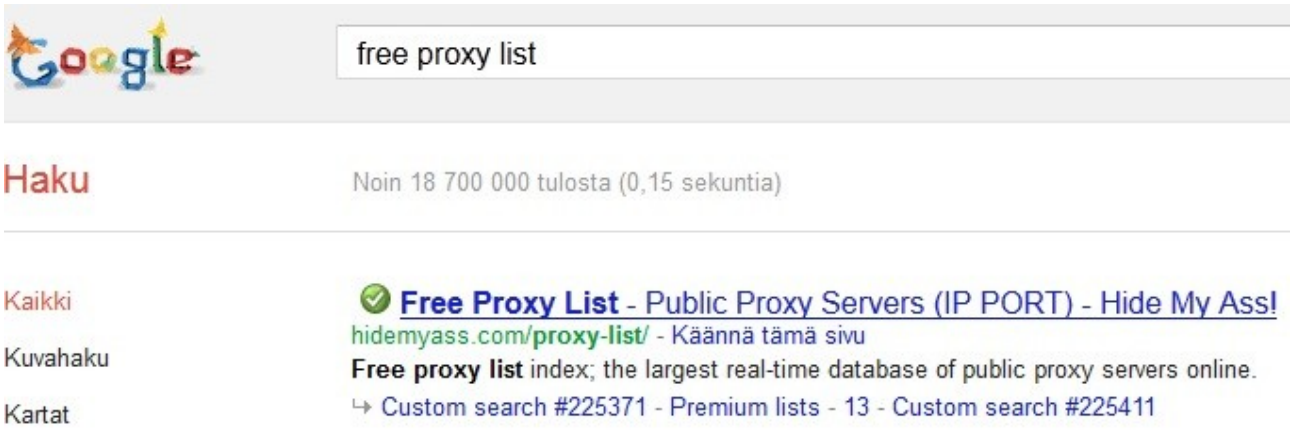
Also activities like wlan-mapping and checking for physical access is considered part of recon activities and often they provide a backdoor to intranet of a organization.

Reconnaisance using Google Hacking

Google hacking is much used method for gaining more information about target system. The Google hacking is basically a method for making detailed and targeted queries in Google. It does not mean hacking attempts against Google as some people might think.
Even tough Google hacking is legal, it poses a slight problem for Google servers. This is because hackers have made automated tools for Google hacking. For example to find certain vulnerabilities from Google. This will generate a extra traffic to Google servers and because of this Google has taken actions against automated Google hacking attempts. So if some one makes a lot of Google queries (queries that are suspicious) in a short time, Google will start to limit the traffic. Google will also make efforts to identify whether it is a human or a automated tool that is making those queries by using captcha.

For this reason we have to hide our IP-address from Google. Since if 20+ students start to make Google hacking queries from a common metropolia IP-address (remember NAT), it will look like a automated Google hacking tool for Google. Google might in this case ban Metropolia's network from using Google. It is not a problem if you make Google queries in your home, because you are the only one making those queries.

To hide our IP-address we have to use proxies. To find Web/Cgi proxy we can use Google:



Use one of these proxies and make sure that your IP is hidden. You can check your IP from services provided by several sites. Do the checking before and after you use the proxy:

After successfully hiding your IP consider shortly following questions:

- What are the risks when using proxy for web surfing and other activity?
- What kind of services proxies provide for you?
- What kind of proxy would be ideal and what kind of services it would have?
- Is having a proxy enough to protect your privacy? What other steps you could take to make sure that you don't get caught?

Once you get your proxy working move on to next phase.

Using Google

Basic Google hacking methods include following:

- To force google to include some search terms use the + sign
- To force google to exclude some search terms use the – sign
- To search exact phrase, use "" signs

Usually attackers want to limit their recon activities to certain organization. This can be achieved using the Google site-operator. To limit searches to Metropolia's websites you can use:

Remember that there should not be any spaces between *site:* and *metropolia.fi*.
Site-operator requires search terms to be included also. Site-operator just limits the search to Metropolia, but Google has to know also what are you searching. In example above "project work" is the actual search term.

One of the most used Google tricks is the "index of"-trick. "index of" is visible in directory listings of the website. Often these directory listings are unintentional and can reveal a lot of information about organizations or people. The "index of" is usually combined with the site-operator as is done in following example:

You can now amuse yourself by searching students and teachers directory listings. You can also try out these in other organizations too (but just to be sure don't start browsing NASA or Nordea even tough you could).

Google hacking is once again more art than skill and you have to learn it by doing. Searching for vulnerabilities and misconfigured servers is based on knowing what kind of pages certain applications and servers generate. For example if you want to find default apache installation with default passwords from Google, you would have to investigate what kind of webpages are in default installation of apache (Welcome to Apache? Or something similar.) Or if you want to find webcams from Google, you could find out the default admin page of certain webcam. What texts there is in that page? Search for those and you could find your webcam.

One good place to start learning is the Google hacking database
http://www.hackersforcharity.org/ghdb/

Go to Google hacking database and try out different google hacking queries to Metropolia's network. You can try out also those in other parts of Internet.

If you find something illegal or information that should not be accessible from Metropolia's network, teacher will give you points for better grade.

Remember searching Google is legal, but if you exploit what you find you just might have committed a crime.