

Exercise 2. Network scanning

In this exercise you can work on groups if you wish. Each group should return a short lab report (1-2 pages) about their findings. When the lab report is returned, the lab is considered done. You should submit your lab-report to Tuubi.

So we will try to find as much information about Metropolia network as possible. We will use this information when trying to scan and find weak points in intranet.

Metropolia's network should be so well built that it is protected against intranet attacks. So any attempts from normal classrooms should not be successful.

So before launching any scanning attempts we want to know exact network topology of network.

So use following means to find out network topology and names of computers/servers.

- google hacking
- examining the support pages
- nslookup
- whois queries (arin & ripe)
- find out all nameserver and see if they let us do zone transfers
- ping, telnet & web-access to ip-addresses

Scanning the Metropolia's network:

Read this:

SCANNING IS ILLEGAL!!!

But this time we have special permission to scan Metropolia's network range.

In this exercise you will scan open services of the school network. You can use any tool, **but make sure that it does not exploit the target once a vulnerable service is found.**
ALSO MAKE SURE THAT YOU SCAN METROPOLIA NETWORK!!!!

Checking Metropolia's network range:

This can be done by using whois services that can be found from Internet. There are several different possibilities to do this. Some of them gives you very nice information about the target. A basic way:

1. Find out the IP-address of Metropolia (nslookup www.metropolia.fi)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\kimmosa>nslookup www.metropolia.fi
Server: kotiboksi.Elisa
Address: 192.168.100.1

Non-authoritative answer:
Name: www.metropolia.fi
Address: 195.148.144.10

C:\Users\kimmosa>
```

2. Go to RIPE (registry of internet names) website www.ripe.net and make whois query with the IP-address that you found in phase one.



The image shows the RIPE Database search interface. It features a search bar with the IP address "195.148.144.10" entered. To the right of the search bar is an orange "Search" button. Below the search bar, there is a disclaimer: "By pressing the 'Search' button you explicitly express your agreement with the RIPE Database Terms and Conditions." At the bottom right, there is a link to "RIPE DATABASE SEARCH" with a right-pointing arrow.

Press the search button and there you have your results:

Search results

This is the RIPE Database search service.
The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.
See <http://www.ripe.net/db/support/db-terms-conditions.pdf>


```
inetnum:      195.148.144.0 - 195.148.151.255
netname:      METROPOLIA-NET
descr:        Helsinki Metropolia University of Applied Sciences
descr:        Metropolia Ammattikorkeakoulu
country:      FI
admin-c:      JK3278-RIPE
```

So now once we have the address range we could go on and make some unsilent scanning activities, but before going there lets make more some silent scanning activities.

Using Nmap:

One tool that could be used is nmap, which you can find from <http://nmap.org/>.

Make sure that you download the latest command line tool since you don't have permissions to install anything into school's computers. Many of the lab computers are missing the WinPcap and if this is the case for your computer, you can not run nmap. In this case you should use virtual computer and install winPcap and nmap there.



The Nmap executable Windows installer also includes the Zenmap graphical frontend.

Latest development release self-installer:
Latest stable release self-installer: [nmap-5.51-win32.exe](#)

We have written [post-install usage instructions](#).

For those who prefer the command-line zip need to run `nmap.exe` from a DOS/command window. Or you can download a [Visual C++ Redistributable Package](#) installers which are included in the zip file.

Latest development command-line zipfile: [nmap-5.61TEST5-win32.zip](#)
Latest stable command-line zipfile: [nmap-5.51-win32.zip](#)

Nmapwin installer:

Usage:

Because it is a command line tool you should open command line tool of Windows. If you still don't know how to do that, you should search Google to find an answer and don't tell anyone that you didn't know...

Lectures told you about what you can search and how, but if you are still confused you should read the basic of scanning from <http://nmap.org/book/man-port-scanning-basics.html>. That should clear your thoughts a little bit. Remember that scanning is a skill that needs to be learned by doing.

Now there are several ports that we could be interested in but you probably are interested in f.e. Web-ports (port 80, 8000, 3000) since a lot of devices have a web interface to change settings. These ports are usually located at 80 but also 8000 and 3000 have been seen.

Netbios ports (135,139,445) are also interesting since you could map a windows share from a computer and access all the files of that computer. In Metropolia network that is nowadays blocked quite well so I would not count on finding much there. In the Internet however netbios ports are scanned a lot.

Remember scanning is considered illegal and you should not practice it on live networks without permission!!!