**Basic Knowledge Assignment**

**Made by** Tim Chermin

**Version:** 1.1

**Date:** 20/09/2019

Table of Contents

[Version 4](#_Toc19883349)

[Introduction 5](#_Toc19883350)

[Subjects 5](#_Toc19883351)

[Networking 5](#_Toc19883352)

[Relevance 5](#_Toc19883353)

[Starting point 5](#_Toc19883354)

[Approach 5](#_Toc19883355)

[Background information 6](#_Toc19883356)

[Law, Ethics and Responsible Disclosure 7](#_Toc19883357)

[Basic Hacking Process 7](#_Toc19883358)

[Relevance 7](#_Toc19883359)

[Starting point 8](#_Toc19883360)

[Approach 8](#_Toc19883361)

[Background information 8](#_Toc19883362)

[Execution 10](#_Toc19883363)

[Afterthoughts 10](#_Toc19883364)

[Sources 10](#_Toc19883365)

[Social Engineering and Foot printing 10](#_Toc19883366)

[Basic challenge 10](#_Toc19883367)

[Network Scanning and Enumeration 19](#_Toc19883368)

[Network Sniffing and Spoofing 19](#_Toc19883369)

[SQL Injection 20](#_Toc19883370)

[XSS 20](#_Toc19883371)

[CSRF 20](#_Toc19883372)

[Path Traversal, File inclusion and Command Injection 21](#_Toc19883373)

[Password Cracking (system and network) 21](#_Toc19883374)

[Wireless Hacking 21](#_Toc19883375)

[Tooling (VMWare ESX and Seclab, Wireshark, Linux basic skills, Web application Proxy & browser tools) 22](#_Toc19883376)

[Linux basic skills: 22](#_Toc19883377)

[Wireshark: 26](#_Toc19883378)

[Final Conclusion and Reflection from the first ten weeks 27](#_Toc19883379)

[Bibliography 27](#_Toc19883380)

# Version

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Autor** | **Date** | **Changes** | **Time spend** |
| 1.0 | Tim Chermin | 13/09/2019 | * Basic setup * Start of Basic Hacking Process added * Start of Linux added | 10 hours |
| 1.1 | Tim Chermin | 19/09/2019 | * Start of Networking * Updated Linux | 8 hours |
| 1.2 | Tim Chermin | 20/09/2019 | * Start of Network Scanning and Enumeration * Start of Network Sniffing and Spoofing * Start of Foot printing, Reconnaissance and Social Engineering * Wireshark | 10 hours |
| 1.3 | Tim Chermin | 21/09/2019 | * Finished Foot printing, Reconnaissance and Social Engineering | 4 hours |

# Introduction

Before this semester I had 0 prior knowledge and experience on security, Linux and networking. Because of this my preferred learning style is the style for beginners (style 1). In this document I’m hoping to learn as much of the basics as I possibly can.

Right now, this document has a lot of template things still in it but I would like to point to the Basic hacking process and the Linux section.

# Subjects

## Networking

### Relevance

The networking basics are needed in this whole basic knowledge assignment. Without knowing these basics, it would be extremely hard to complete this assignment.

### Starting point

My prior knowledge concerning Networking:

At this point I haven’t done any research on networking yet. So, my knowledge is close to nothing.

### Approach

I started with following the instruction about this subject and after the instruction I gathered the information I gained and use it to do some more research about it on the internet.

### Background information

ARP, IPv4, ICMP ping, TCP/IP, DNS, HTTP, FTP, SMTP

**IP(v4/6) and MAC:**

An IP Address or Internet Protocol address is a numerical label assigned to each device that’s connected to a network which uses the IP for communication. IP addresses have two principal functions. It identifies the network interface (host) and it provides the location of the host in the network. (IP\_address, 2019)

A MAC address is the physical address of the device and is often assigned by the manufacturer.

**Routers:**

Network infrastructure is something that is used to provide network services that allows other devices to connect and communicate.

For example, Routers can connect multiple devices (for example client and servers) and networks together by forwarding traffic. This is how data gets from one place to another on something like the internet. Routers enable all networked computers to share a single internet connection.

Routers act like a dispatcher, it gathers and analyses data that’s being sent across the network. It then chooses the best route for the data to travel and sends it on its way. In the image to the right, you can see an example of the different paths data could take. (NetworkingBasics, n.d.)

Each package of data contains 2 IP addresses, 1 of the sender and 1 of the destination. When routing data the IP address of the package won’t change but the MAC address will. (BasicNetworking, 2019)

Figure 1: https://portal.fhict.nl/Studentenplein

**Access Points:**

Access points allow devices to connect to a wireless network, this makes it easy to bring new devices online. An access point is like an amplifier to your network. This means that access points extend the bandwidth that the router provides, so that the network can support more devices and from further away. (NetworkingBasics, n.d.)

**NAT:**

The main use of NAT is to limit the number of public IP addresses an organization can use. (nat, 2019) NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

**DNS:**

The Domain Name System is the phonebook of the internet. (what is dns, n.d.) We access information through domain names like wikipedia.com. DNS translates domain names to IP addresses, because of this browsers can load internet resources.

**Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hand on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Law, Ethics and Responsible Disclosure

 Per **Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hand on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Basic Hacking Process

### Relevance

When you are going to try to hack something you should always keep the process of it in mind. You’re not going to start with the SQL injection, but you’re going to start with finding a target and gathering information about that target. If you forget to gather information about your target, it is going to be a lot harder to hack the target in the end. For that reason, it is a relevant subject for a security professional.

### Starting point

My prior knowledge concerning the basic hacking process:

At this point I haven’t done any research about hacking yet. But using common knowledge I can understand that you would have to start with researching a target before hacking the target.

### Approach

I started with following the instruction about this subject and after the instruction I gathered the information I gained and use it to do some more research about it on the internet.

### Background information

A summary about the basic hacking process injection based on online reading:

In general, a hack is performed in five steps. This is also referred to as the anatomy of a hack. Others call it a hacking methodology: a step-by-step approach to perform a pentest (penetration test) some of these steps only apply to specific types of hacks.

for an ethical hacker there also needs to be a pentest contract! Because of the cyber-crime law, for risks and confidentiality there should always be a signed contract before the hacker starts any testing. A complete pentest contract will need:

* An indemnification clause that allows the hacker to test and address liability. It is necessary to agree to that, even though the tester is responsible for testing carefully, any other risks in testing is for the client. This means that testers are not liable for any damages caused by testing.
* a confidentiality agreement (signed by all testers). This will prevent testers from exposing data of the client.
* information about the scope and tested systems and environments (location, ip-range, dns names, etc.).
* test origin (ip-address from where tests will be performed) and test times/period of testing so that the client can monitor the testing and in this way the client would be able to distinguish real attacks from the tester’s tests.
* escalation procedure in case of an incidents/emergency.

After the contract has been made the ethical hacker can start with the hack. A non-ethical hacker will probably skip the contract and go straight to the next 5 steps.

1. **Intelligence gathering:** The first phase is all about gathering information about the target. When gathering information about your target you’re looking for things like, telephone-numbers, names, email addresses, websites, etc. In this phase you should try to learn as much as possible about a targeted organization before test has even begun. If the hacker would skip the first steps, then it would be close to impossible for him/her to hack the target.

2. **Footprint:** This phase includes the usage of tools like nmap, diallers and vulnerability scanners to scan data. You will try to get an idea about the things like, IP ranges, active ip addresses, open ports and important servers.

3. **vulnerability** **analysis:** Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. Network sniffing (sniffing = "Vulnerability Analysis") is also a part of this phase. Sniffing can be seen as eavesdropping between digitally communicating targets. This can be things like the traffic between a smartphone and an access point or a browser and a webserver on the internet.

The gathered information by sniffing could be valuable on its own but it can also be used to gather even more information. Sniffing won’t alter the sniffed data, but it can be used to impersonate the target, and in that way make a impersonate request to the server (phase 4). One of the tools I will be using for sniffing network traffic (both wired and wireless) is Wireshark.

4. **Exploitation:** The exploitation phase is all about entering the target by using found weaknesses. With the use of Password cracking or a tool as Metasploit. These tests could even cause disruption of services and are often not executed. This phase also uses something called spoofing, spoofing is the act of pretending to be another person or system. For example, the hacker could send an e-mail with a “from” address that isn’t yours. You could also use a technology called ARP spoofing, ARP is a protocol used by everything connected to a network. With this technology you could match IP addresses with the corresponding MAC addresses. This means that you could obtain all of a targets network traffic by pretending you are the router on the network.

5. **Post Exploitation**: post exploitation contains actions such as actual extracting, editing and removing data or adding accounts/backdoors. This phase also contains the clean-up, when a hacker tries to cover his or her tracks, he would be clearing logs and removing evidence. And once a hacker has gained access, he would want to keep that access so that he or she could launch additional attacks. And prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. This way it would be even harder for the target to find the hacker.

**Reporting and delivery: (for ethical hackers)**

The pentest results are delivered in a presentation and a report that will explain all the findings in the test. In the presentation the tester will explain all his findings and conclusions in front of the client. While the report will contain the coals and the scope of the test, an explanation of the test approach, the results of the test and overall conclusions. These conclusions also include advise on how to solve some of the issues.

**The differences and similarities between a pent-test methodology and the cyber kill chain:**

**Similarities:**

* Intelligence gathering
* Exploitation

**Differences:**

* Installing malware
* Fishing mail

### Execution

### Afterthoughts

When I started, I didn’t really understand the different steps of a pentest but after my research it’s gotten a lot clearer. I also think this information is going to help me with my further research on the other subjects.

### Sources

<https://www.geeksforgeeks.org/5-phases-hacking/>

<https://fhict.instructure.com/courses/8790/pages/reference-basic-hacking-and-pentesting-proces?module_item_id=394575>

<https://fhict.instructure.com/courses/8790/pages/reference-footprinting-reconnaissance-and-social-engineering?module_item_id=394577>

<https://fhict.instructure.com/courses/8790/pages/reference-network-scanning-and-enumeration>

<https://fhict.instructure.com/courses/8790/pages/reference-network-sniffing-and-spoofing?module_item_id=394579>

## Social Engineering and Foot printing

### Relevance

Foot printing is a vital part of a pentest, when a hacker skips the foot printing part of the pentest it will be close to impossible to hack the target. Social engineering can help with the foot printing when trying to get information about your target.

### Starting point

I did know tiny little things about Social engineering, but I knew close to nothing about foot printing before this. I only knew a little about Social engineering because a student told me about it last year.

### Approach

I started with following the instruction about this subject and after the instruction I tried the basic challenge as a starting point. After the challenge I gathered the information I gained and used it to do some more research about it on the internet.

### Background information

"**Social engineering** or social hacking, in the context of information security refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick. for the purpose of information gathering, fraud, or system access.” (footprinting reconnaissance and social engineering, n.d.)

**Computer based social engineering: Phishing** is a technique typically used when the hacker sends an email that appears to come from a legitimate business or person. This mail usually contains a link to a fake web page that might look legitimate. On this web page there could be a form that requests every detail about the persons life, it will ask for credit card numbers or other bank information.

**Human based social engineering: Impersonation** is when the hacker impersonates the role of someone who is likely to be trusted. For example, when the hacker would act as someone from KPN. And would then go to a big company with lots of people working on a location. The people would trust the hacker because he acts like someone from KPN, this will give him access to lots of information about the company.

**Foot printing**: "Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system" (footprinting, 2019)

Some of the information that can be gained when foot printing is: Domain names, network blocks, network services and applications, system architecture, phone numbers, contact addresses, specific IP addresses, intrusion detection system.

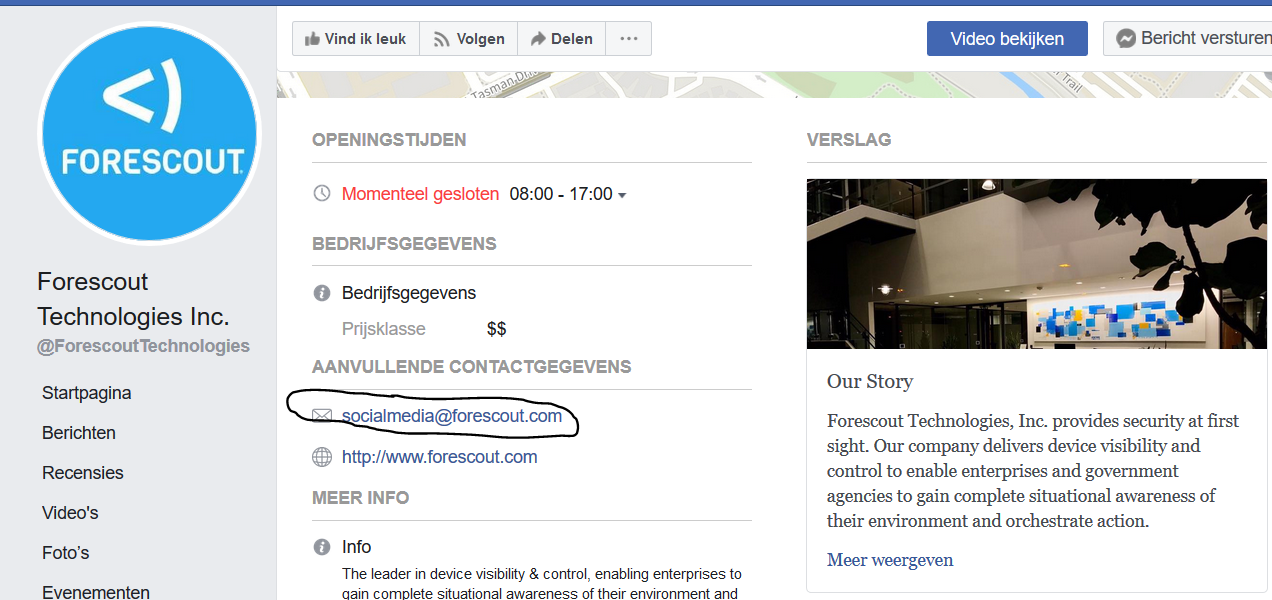
To gain this information the hacker uses different types of tools. But when researching for information the hacker doesn’t have to start with typing some commands in. A simple google search could gain the hacker a lot of information about a company. But after that the hacker would have to use tools like, whois, NSLookup and sam spade.

### Execution

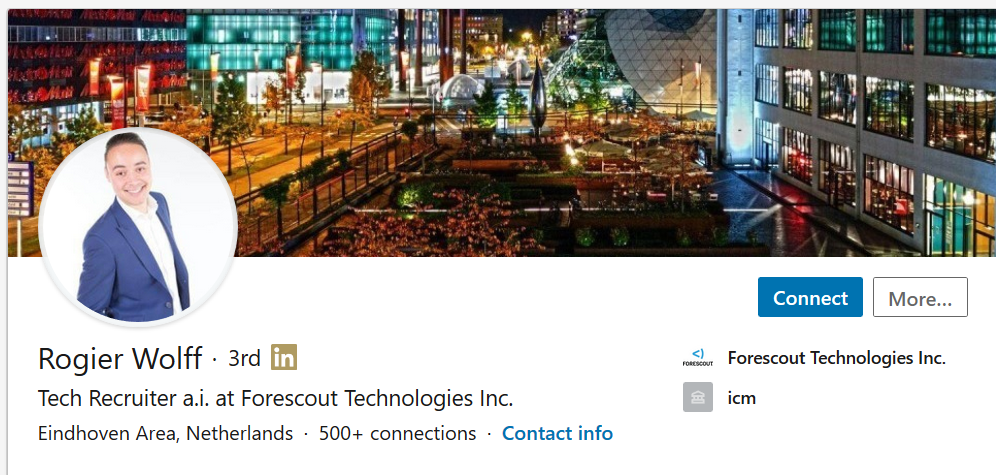
#### Basic challenge

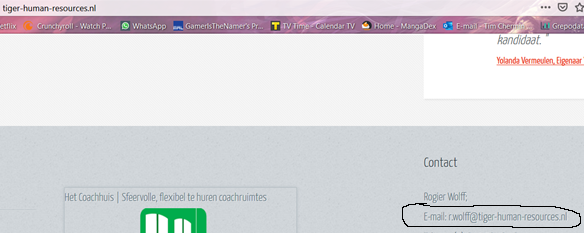
Find at least 3 people including email address (not management) which work with secmatters.com using social networks like LinkedIn.

I found the first mail on Facebook when just going to the Forescout account.

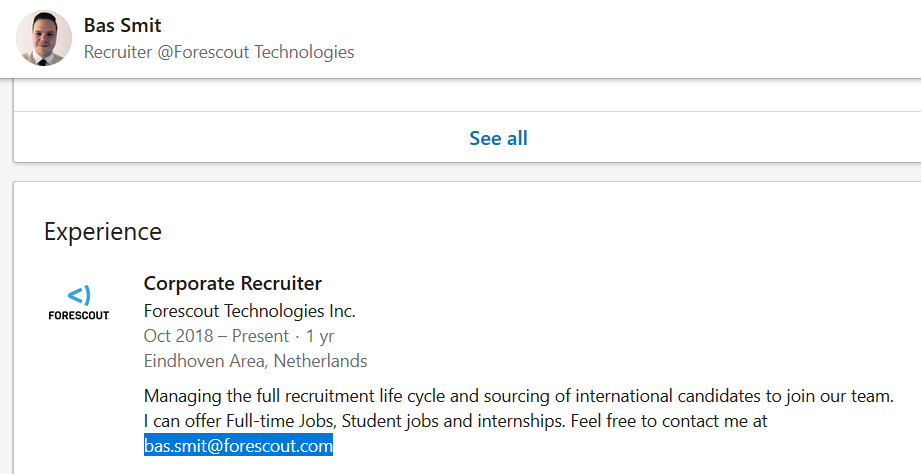


After doing some research I found a mail address on the website of an employee through his twitter.





And I also found a mail on A LinkedIn account of an employee.



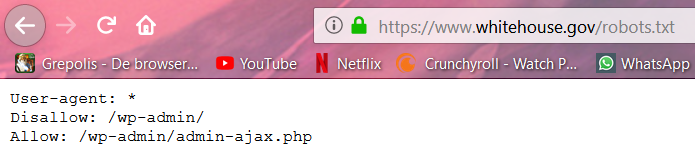
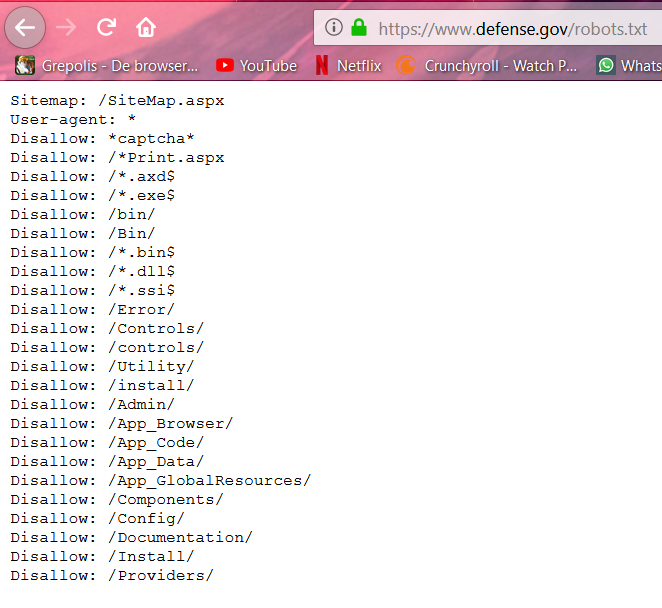
**Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org.**



In the image on the left you can see the front page of 10 years ago, and on the image on the right you can see the frontpage of today (20/09/2019).

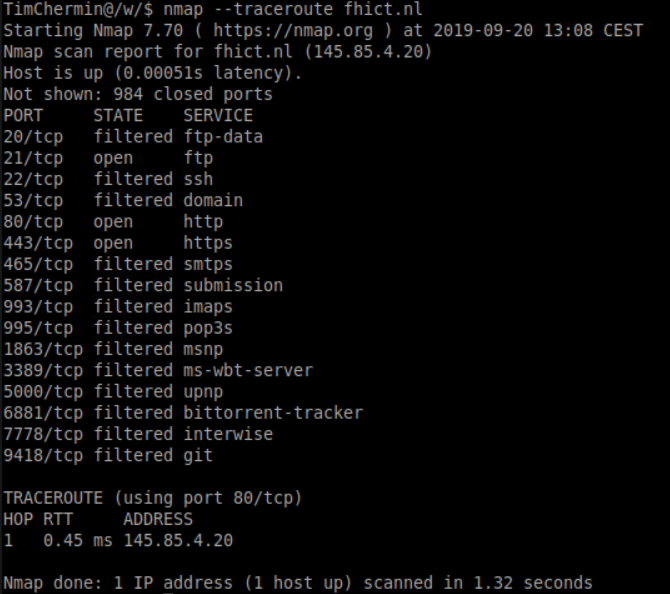
**Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.**

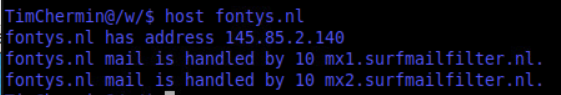
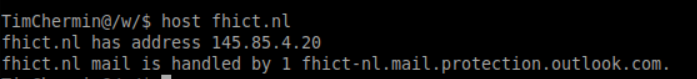
At first, I had no idea what robot.txt was but after a quick google search I found these results. “Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called The Robots Exclusion Protocol.” (robotstxt, n.d.)



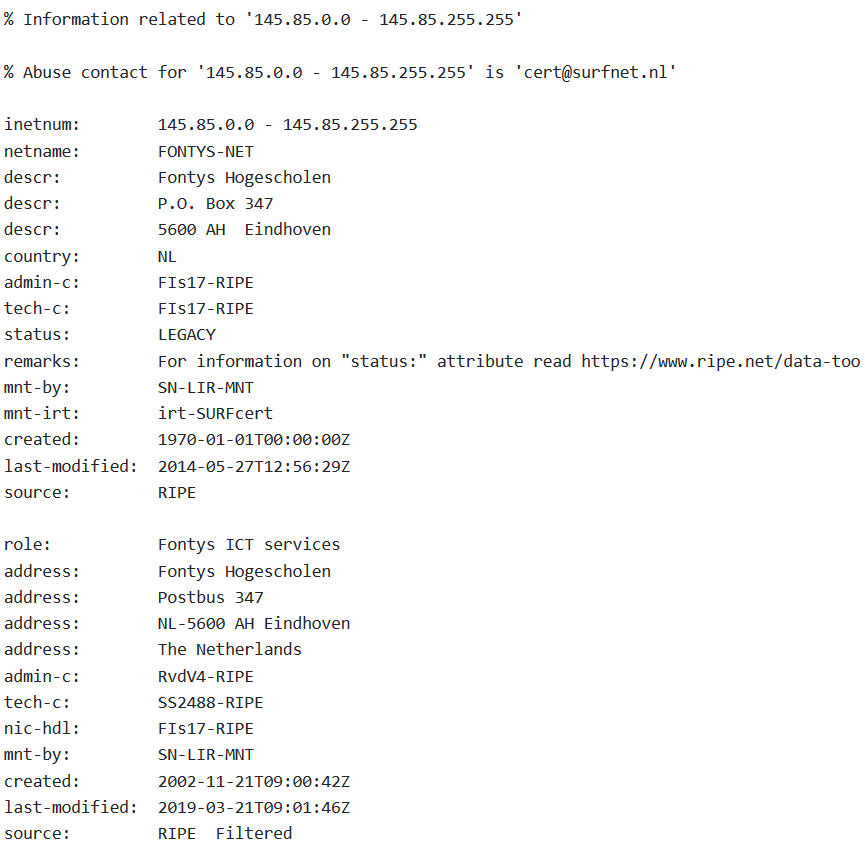
**Use kali for traceroute to determine path to fontys.nl, fhict.nl.**

Since I tested this with the cisco any connect VPN the path is obviously not long at all.

 (Raymond, 2013)

**Determine which DNS and email servers are used by Fontys and fhict.**(SecurityTrails team, n.d.)

**Determine which ip-addresses are used by fhict by whois utility and non whois tool**



**Run theharvester utility for domain fontys.nl.**

**having no idea what theharvester was going to do I just tried the command and it gave me a list of options. After that I only needed to fill in the examples with my own to get information about fonys.nl. The results gave me all the information I needed to know what theharvester does.**



### Afterthoughts

When I started, I didn’t really understand the different steps of a pentest but after my research it’s gotten a lot clearer. I also think this information is going to help me with my further research on the other subjects.

## Network Scanning and Enumeration

### Relevance

Scanning a network can help to give the hacker a better understanding of an environment.

### Starting point

I didn’t know anything about scanning and enumeration before this assignment.

### Approach

I started with following the instruction about this subject and after the instruction I gathered the information I gained and used it to do some more research about it on the internet.

### Background information

Scanning is the process of locating systems that are alive and responding on the network Ethical hackers use scanning to identify target systems IP addresses. Scanning is also used to determine where a system is on the network.

**Port scanning with Nmap:**

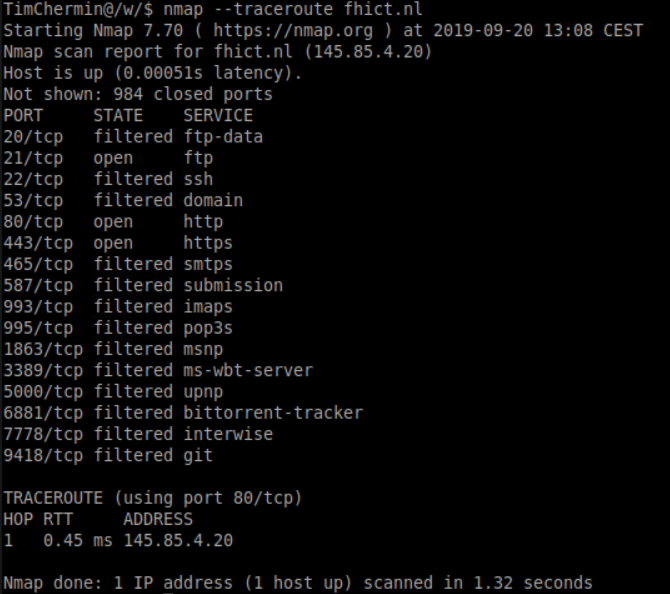
Nmap is a free open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, Ip address detection and operating system detection.

There are 2 types port scanning (ports and services), **network scanning** (identifies IP addresses on a given network or subnet), **vulnerability scanning** (discovers presence of known weaknesses on a target system)

port numbers are divided into three ranges:

* Well know ports 0-1023
* Registerd ports 1023-49151
* Dynamic ports 49152-65535 used on client side

For example, FTP has 21, telnet has 23 and http has 80. In the image bellow you can see the different ports.



**TCP:**

**The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.**

Scanning methodology:

NMAP scantypes: TCP connect, XMAS tree scan, SYN stealth scan, NULL scan, Windows scan, ACK scan.

Banner grabbing and OS fingerprinting techniques: Active stack fingerprinting, passive stack fingerprinting. TOOLS: netcraft and HTTTtrack

Scanning anonymously: preparing proxy servers is the last step in the CEH scanning methodology. A proxy server is a computer that acts as an intermediary between the hacker and the target computer. Using a proxy server can allow a hacker to become anonymous on the network.

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services.

Hacking tools: dumpsec, hyena, the smb auditing tool, the netbios auditing tool.

SNMP enumeration: is the process of using SNMP to enumerate user accounts on a target system.

* Read and understand how a tcp communication session is set up
* Then read and understand the different type of portscanning techniques: [https://nmap.org/book/man-port-scanning-techniques.html (Links to an external site.)](https://nmap.org/book/man-port-scanning-techniques.html)
* Also read about the different results you can get for a tcp (or udp) port: [https://nmap.org/book/man-port-scanning-basics.html (Links to an external site.)](https://nmap.org/book/man-port-scanning-basics.html)
* Read about service scans for enumeration: [https://nmap.org/book/man-version-detection.html (Links to an external site.)](https://nmap.org/book/man-version-detection.html). Besides using nmap service scans also use telnet or client software ((ftp client, ssh client, browser to port 80/8080/443, etc.) to connect to certain ports to receive banner or other typ of information about the software running behind a certain port.
* Read about how you can detect the operating system of a system: [https://nmap.org/book/man-os-detection.html (Links to an external site.)](https://nmap.org/book/man-os-detection.html)
* Conclusions towards a standard scanning and enumeration process:  
  - In a portscan you might want to start with the default syn-scan on the 1000 most well-known ports.  
  - Depending on the port results being closed/filtered/unfiltered you might try other types of portscans.  
  - For systems that might be interesting you perform an Operating System scan (nmap -O option) and you scan all tcp port (nmap -p- option), and all udp ports (nmap -sU option), perform a service scan (-sV) on ports that you further want to investigate.  
  - Manage your time well, some scans might take a long time. Go from faster quick scans on networks where you are 'blindfolded' to complete and more intense scans on targeted machines. Read the possibilities in [https://nmap.org/book/man-port-specification.html (Links to an external site.)](https://nmap.org/book/man-port-specification.html), e.g. consider the -F option when scanning larger ip-ranges such as a class B (/16) subnet.

**Challenges**

Deploy a Kali machine in your assigned VLAN (see links below for eventual instructions), and then:

Perform different NMAP scans to other VLANs. For VLAN200 (Management Network), mind the network load as mentioned before so NEVER intense scan on machines in VLAN200. Better deploy an old template and scan in your own (private) VLAN. Use [Reference] Wireshark tool to see and understand what's exactly being scanned

For all found IPs, provide a description of what you found and whether you can find potential security issues.

Other scanning tools are OpenVAS and Nessus. Deploy some test target machines in your VLAN and install some software of your choice.

Then scan with NMAP, OpenVAS and Nessus in this network and describe the results

Try out different settings of all tools and see what different results you get and why this is the case.

Try metasploit (only in this test environment) and see if you can really exploit a vulnerability.

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Network Sniffing and Spoofing

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## SQL Injection

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

‘OR ‘1’ = ‘1

1 is altijd gelijk aan 1. Dus haal gegevens op voor iets OF 1=1

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## XSS

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## CSRF

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Path Traversal, File inclusion and Command Injection

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Password Cracking (system and network)

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Wireless Hacking

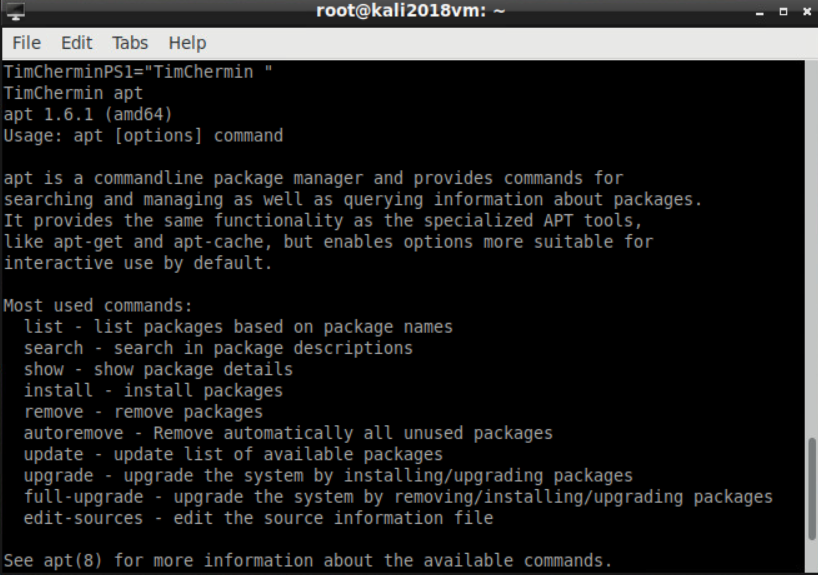
 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

## Tooling (VMWare ESX and Seclab, Wireshark, Linux basic skills, Web application Proxy & browser tools)

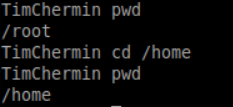
### Linux basic skills:

**Command line activities:**

**APT:** 

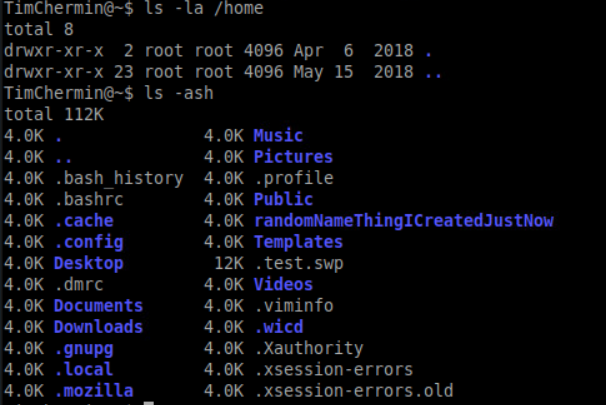
The CLI's apt command lets you search for, install, and remove software and add new repositories.

**Pwd:**

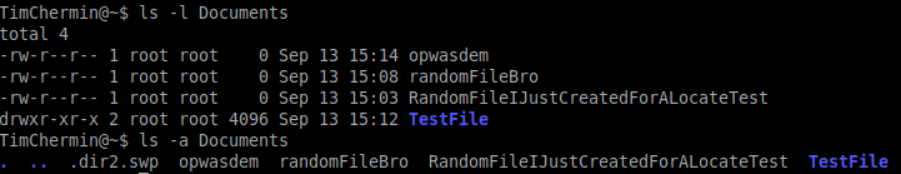


Use the pwd command to print the working directory (the current directory you are in).

**ls -la /home**

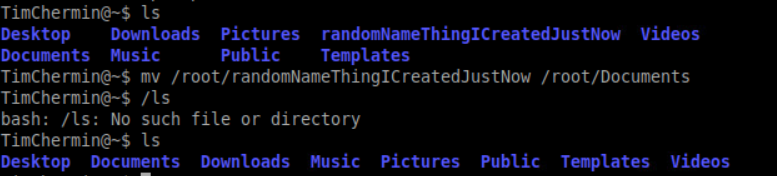


Lists ALL the files and directories in the /home directory, in the long listing format.

**Ls -ash**

Lists ALL the files in the current directory (no directory was specified so it lists the contents of the current directory), and the size of the files/directories, written in 'human readable' format.

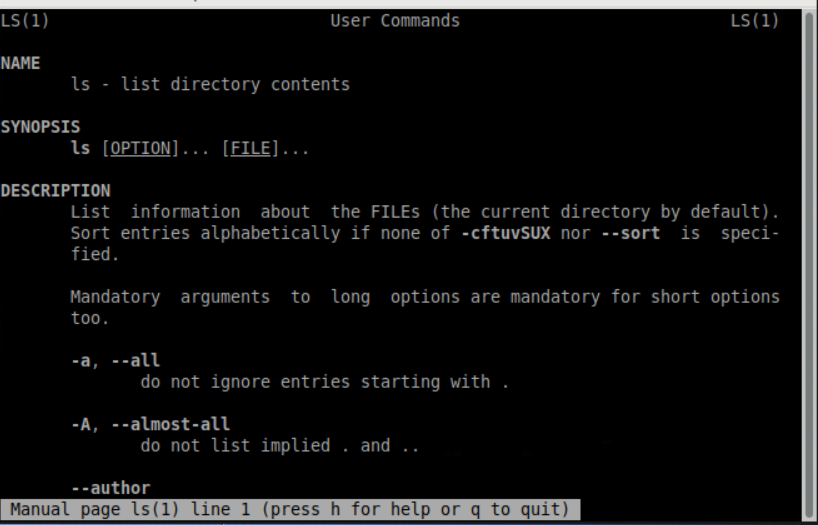
**Mv:**



The mv(move) command allows a user to move a file to another folder or directory.

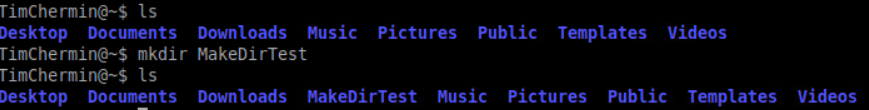
**Man:**

**Man ls:**

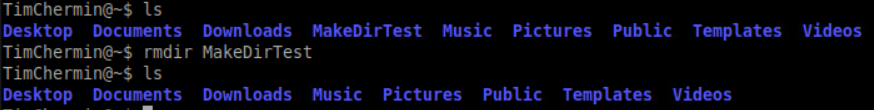


The manual command shows the manual of the inputted command.

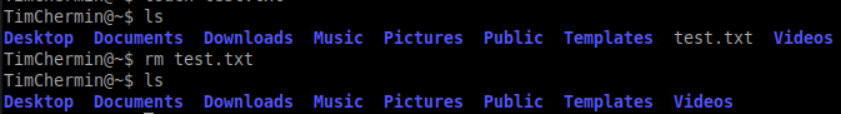
**Mkdir & rmdir & rm:**



The mkdir(make directory) command allows the user to make a new directory. Just like making a new directory within a PC or Mac desktop environment, the mkdir command makes new directories in a Linux environment.

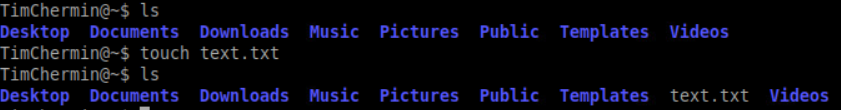


The rmdir(remove directory) command allows the user to remove an existing empty directory.



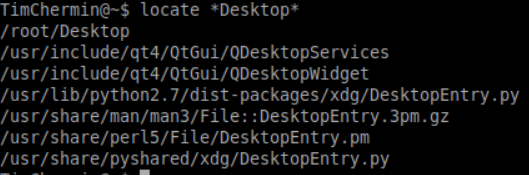
The rm command will remove directories and files held within, the rm command will delete created files.

**Touch:**



The touch command allows users to make files and to change the last used time to the users current time.

**Locate:**



The locate command is meant to find a file, if you don't know the name of a certain file or you aren't sure where the file is saved and stored

Learning and accountability:

1. In your learning portfolio, give a **summary** of your learning activities with some **highlights and explanations**, and an **evaluation** of what you have learned in your learning portfolio.
2. Add **all** your command-line activities (screenshots) in an appendix to your learning portfolio.
3. **Always** change the command-prompt to your name or initials as proof of your personal activity. This can be achieved by changing the PS1 environmental variable, e.g.:

PS1="YourInitials@\w\$ "

1. Make sure you can explain and reproduce most of what you have done at the assessment.

**Sources:**

<http://www.informit.com/blogs/blog.aspx?uk=The-10-Most-Important-Linux-Commands>

<https://fhict.instructure.com/courses/8790/pages/reference-tooling-linux-command-overview>

<https://www.mediacollege.com/linux/command/pwd.html>

<http://overthewire.org/wargames/bandit/>

### Wireshark:

Make sure that you understand the basics for port scanning with nmap, and show for those in your learning portfolio (e.g. by working according to the suggested process):

* Read and understand how a tcp communication session is set up
* Then read and understand the different type of port scanning techniques: [https://nmap.org/book/man-port-scanning-techniques.html (Links to an external site.)](https://nmap.org/book/man-port-scanning-techniques.html)
* Also read about the different results you can get for a tcp (or udp) port: [https://nmap.org/book/man-port-scanning-basics.html (Links to an external site.)](https://nmap.org/book/man-port-scanning-basics.html)
* Read about service scans for enumeration: [https://nmap.org/book/man-version-detection.html (Links to an external site.)](https://nmap.org/book/man-version-detection.html). Besides using nmap service scans also use telnet or client software ((ftp client, ssh client, browser to port 80/8080/443, etc.) to connect to certain ports to receive banner or other typ of information about the software running behind a certain port.
* Read about how you can detect the operating system of a system: [https://nmap.org/book/man-os-detection.html (Links to an external site.)](https://nmap.org/book/man-os-detection.html)
* Conclusions towards a standard scanning and enumeration process:  
  - In a portscan you might want to start with the default syn-scan on the 1000 most well-known ports.  
  - Depending on the port results being closed/filtered/unfiltered you might try other types of portscans.  
  - For systems that might be interesting you perform an Operating System scan (nmap -O option) and you scan all tcp port (nmap -p- option), and all udp ports (nmap -sU option), perform a service scan (-sV) on ports that you further want to investigate.  
  - Manage your time well, some scans might take a long time. Go from faster quick scans on networks where you are 'blindfolded' to complete and more intense scans on targeted machines. Read the possibilities in [https://nmap.org/book/man-port-specification.html (Links to an external site.)](https://nmap.org/book/man-port-specification.html), e.g. consider the -F option when scanning larger ip-ranges such as a class B (/16) subnet.

 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

* What you learned:
  + How is this subject relevant for you as a junior security professional?
  + Do you understand this subject (theory)? (provide evidence, e.g. summary)
  + How did you practice this subject hands on (practical)? (provide evidence, e.g. screenshots including your explanation)
  + What tools and sources did you use? (refer to sources)
  + Results proving that you became (hands on) competent in a subject
* How you learned it:
  + what did you do to become (hands on) competent in a subject?
  + Did you manage to master this subject sufficiently? (conclusion)
  + What are the lessons learned? (reflection on working on the subject)

# Final Conclusion and Reflection from the first ten weeks

Critical reflection on the results of your own learning process thus far.

How was your Pro-active attitude thus far (being present, taking initiative)

How did you communicate with teachers, fellow students, experts (presenting, advising, inquiring and eventual reporting)

# Bibliography

*BasicNetworking*. (2019, September 12). Retrieved from fhict: https://portal.fhict.nl/Studentenplein/LMC/\_layouts/15/WopiFrame.aspx?sourcedoc=/Studentenplein/LMC/1920nj/Cyber%20Security/CSA/000\_Network%20Fundamentals/Basic%20network%20summary%20201809.pptx&action=default

*footprinting*. (2019, July 25). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Footprinting

*footprinting reconnaissance and social engineering*. (n.d.). Retrieved from fhict: https://fhict.instructure.com/courses/8790/pages/reference-footprinting-reconnaissance-and-social-engineering?module\_item\_id=394577

*IP\_address*. (2019, September 18). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/IP\_address

*nat*. (2019). Retrieved from whatismyipaddress: https://whatismyipaddress.com/nat

*NetworkingBasics*. (n.d.). Retrieved from cisco: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html

Raymond. (2013, July 15). *how can i see traceroute details in nmap*. Retrieved from stackexchange: https://security.stackexchange.com/questions/38964/how-can-i-see-traceroute-details-in-nmap

*robotstxt*. (n.d.). Retrieved from robotstxt: https://www.robotstxt.org/robotstxt.html

SecurityTrails team. (n.d.). *domain tools*. Retrieved from securitytrails: https://securitytrails.com/blog/domain-tools

*what is dns*. (n.d.). Retrieved from cloudflare: https://www.cloudflare.com/learning/dns/what-is-dns/

**Competitive intelligence** means information gathering about competitors

DNS information: common DNS record types and use

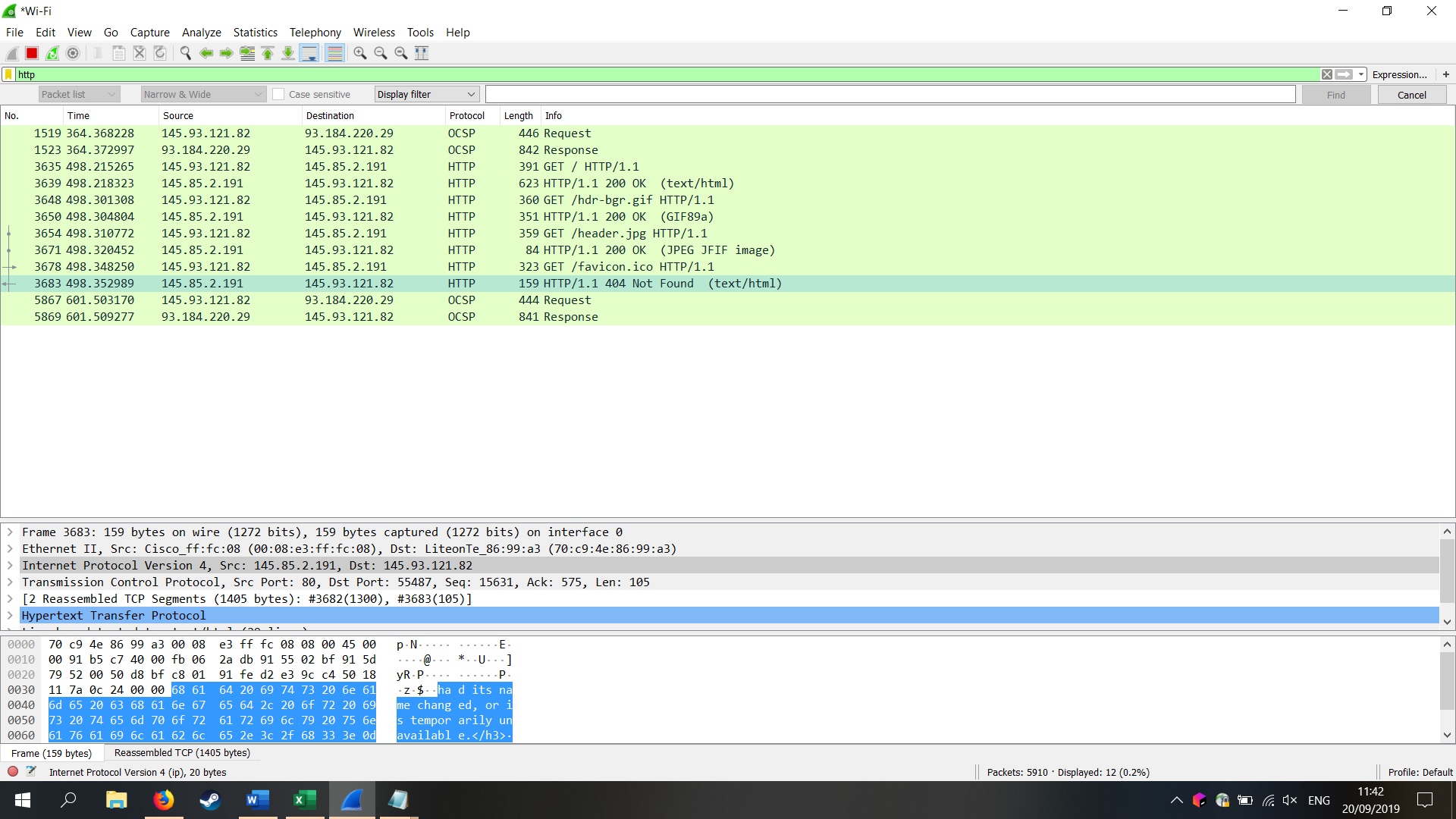
* A(Address) maps a hostname to an IP address
* SOA (start of authority) identifies the DNS server responsible for the domain info
* CNAME (canonical name) provides additional names or aliases for athe address record
* MX(Mail exchange) identifies the mail server for the domain
* SRV(service) identifies services such as directory services
* PTR(pointer) maps IP addresses

Packet tracing tools, NeoTrace, Visual route, VisualLookout

Webspiders: spammers and anyone else interested in collecting email addresses from the internet can use webspiders.

Wireshark: live capture from many different network media, import files from many other capture programs, export files for many other capture programs, many protocol dissectors, open source software.

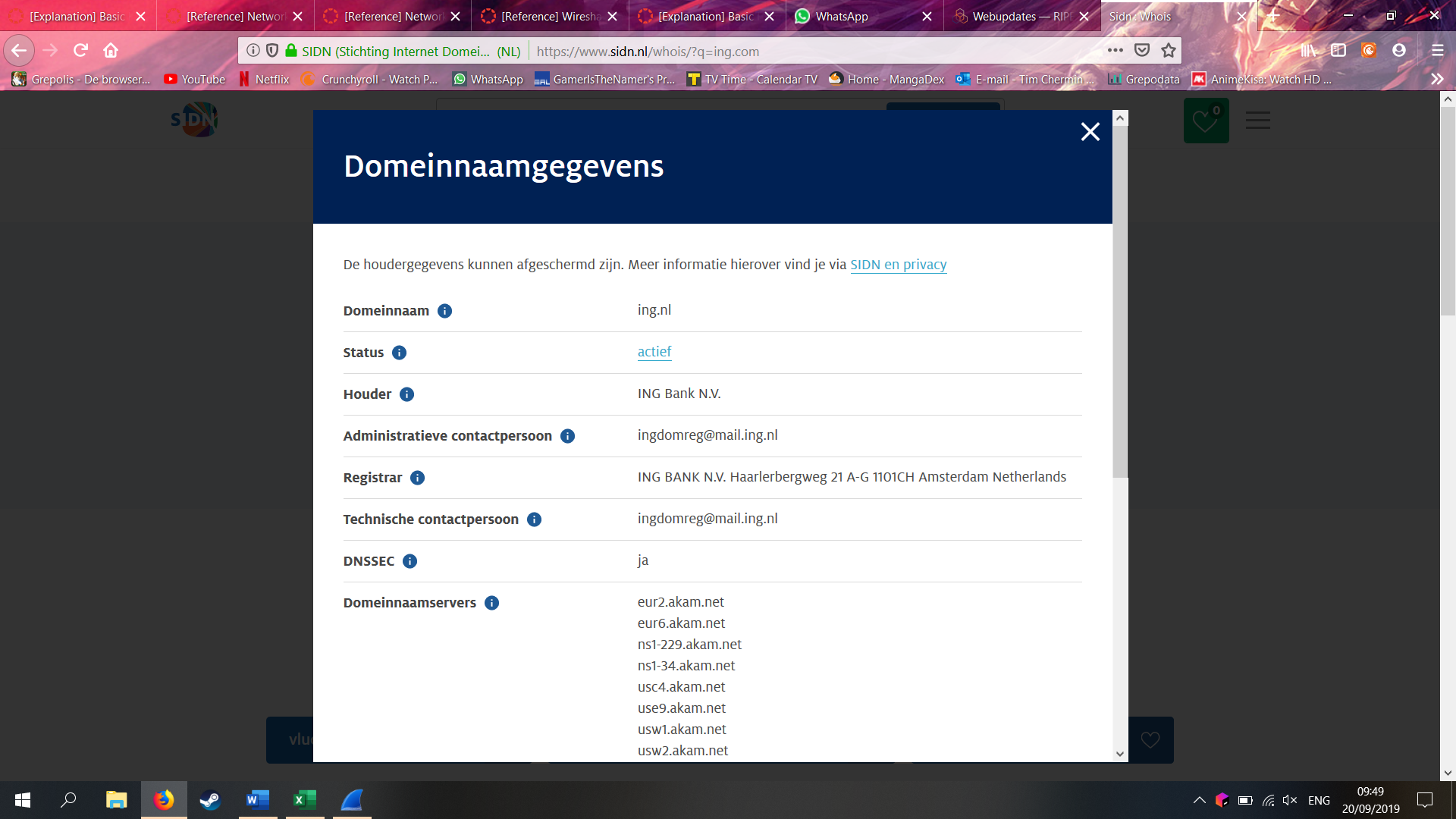
Http-filter <http://merlijnw.freaze.eu/>



<https://www.shodan.io/>

<https://www.ripe.net/>





**Google search engine:** groups.goolge.com to search for newsgroups, site, filetype, link, cache, initle, inurl.

Google dorks: <https://www.exploit-db.com/google-hacking-database> 