**Basic Knowledge Assignment**

**Made by** Tim Chermin

**Version:** 1.7

**Date:** 28/09/2019

Table of Contents

[Version 4](#_Toc20570942)

[Introduction 5](#_Toc20570943)

[Subjects 5](#_Toc20570944)

[Networking 5](#_Toc20570945)

[Relevance 5](#_Toc20570946)

[Starting point 5](#_Toc20570947)

[Approach 5](#_Toc20570948)

[Background information 5](#_Toc20570949)

[Law, Ethics and Responsible Disclosure 5](#_Toc20570950)

[Relevance 5](#_Toc20570951)

[Starting point 5](#_Toc20570952)

[Approach 5](#_Toc20570953)

[Background information 5](#_Toc20570954)

[Afterthoughts 5](#_Toc20570955)

[Basic Hacking Process 5](#_Toc20570956)

[Relevance 5](#_Toc20570957)

[Starting point 5](#_Toc20570958)

[Approach 5](#_Toc20570959)

[Background information 5](#_Toc20570960)

[Afterthoughts 5](#_Toc20570961)

[Sources 5](#_Toc20570962)

[Social Engineering and Foot printing 5](#_Toc20570963)

[Relevance 5](#_Toc20570964)

[Starting point 5](#_Toc20570965)

[Approach 5](#_Toc20570966)

[Background information 5](#_Toc20570967)

[Execution 5](#_Toc20570968)

[Afterthoughts 5](#_Toc20570969)

[Network Scanning and Enumeration 5](#_Toc20570970)

[Relevance 5](#_Toc20570971)

[Starting point 5](#_Toc20570972)

[Approach 5](#_Toc20570973)

[Background information 5](#_Toc20570974)

[Afterthoughts 5](#_Toc20570975)

[Network Sniffing and Spoofing 5](#_Toc20570976)

[SQL Injection 5](#_Toc20570977)

[Relevance 5](#_Toc20570978)

[Starting point 5](#_Toc20570979)

[Approach 5](#_Toc20570980)

[Background information 5](#_Toc20570981)

[Execution 5](#_Toc20570982)

[Afterthoughts 5](#_Toc20570983)

[XSS 5](#_Toc20570984)

[CSRF 5](#_Toc20570985)

[Path Traversal, File inclusion and Command Injection 5](#_Toc20570986)

[Password Cracking (system and network) 5](#_Toc20570987)

[Wireless Hacking 5](#_Toc20570988)

[Tooling (VMWare ESX and Seclab, Wireshark, Linux basic skills, Web application Proxy & browser tools) 5](#_Toc20570989)

[Relevance 5](#_Toc20570990)

[Starting point 5](#_Toc20570991)

[Approach 5](#_Toc20570992)

[Execution 5](#_Toc20570993)

[Final Conclusion and Reflection from the first ten weeks 5](#_Toc20570994)

[Bibliography 5](#_Toc20570995)

# 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 Foot printing, Reconnaissance and Social Engineering * Start of Wireshark | 10 hours |
| 1.3 | Tim Chermin | 21/09/2019 | * Finished Foot printing, Reconnaissance and Social Engineering for now | 7 hours |
| 1.4 | Tim Chermin | 22/09/2019 | * Finished Network Scanning and enumeration for now | 5 hours |
| 1.5 | Tim Chermin | 26/09/2019 | * Finished Linux | 4 hours |
| 1.6 | Tim Chermin | 27/09/2019 | * Start of SQL injection * Start of Law, Ethics and Responsible disclosure. | 7 hours |
| 1.7 | Tim Chermin | 28/09/2019 | * Finished SQL injection * Finished Law, Ethics and Responsible disclosure. | 5 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, networking, Law Ethics and responsible disclosure, network scanning and enumeration, foot printing and social engineering, Wireshark 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 used 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

### Relevance

Knowing what you are doing is legal or illegal is important for a white hat hacker. If you try to do something that’s illegal than you will probably get in a lot of trouble. But if you do everything in a legal way you may even get payed for it.

### Starting point

My prior knowledge concerning Law, Ethics and Responsible Disclosure:

At this point I get that stealing money from a bank through hacking is illegal. While performing a pentest when in an agreement with a company is legal. So, I know I little bit of this subject but not a lot.

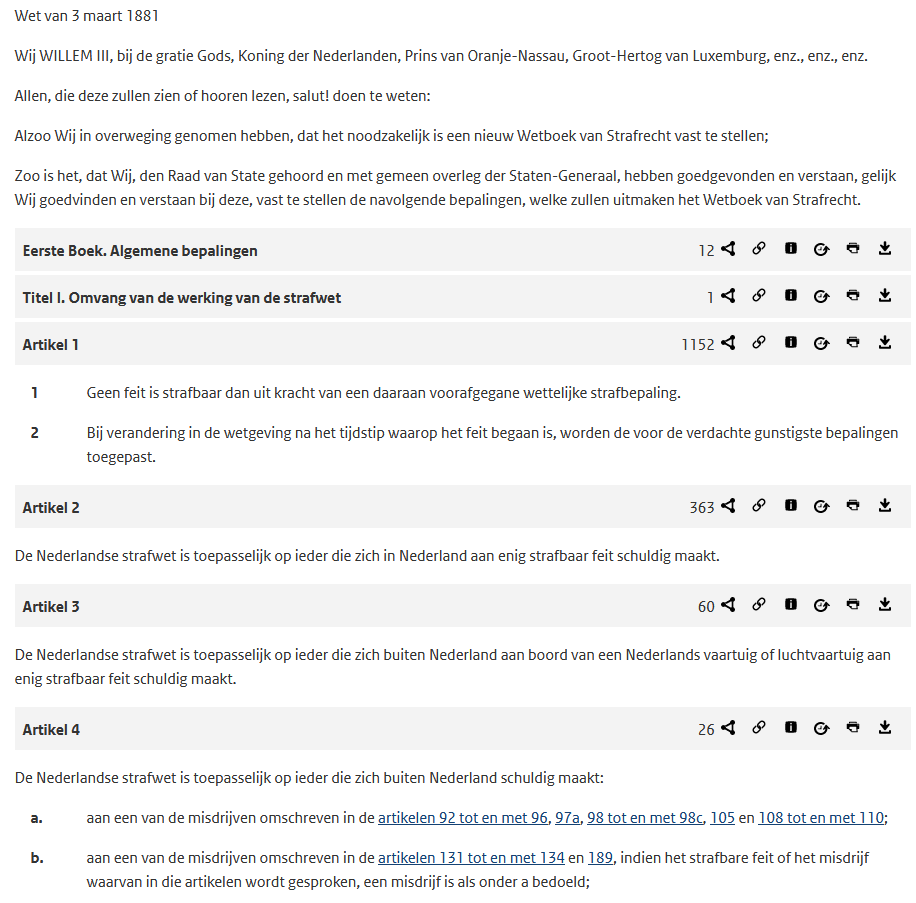
### Approach

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

#### Basic:

**Read in the convention on cybercrime which forms of cybercrime are defined in article 2-13.**

 (Wetboek van strafrecht , n.d.)

Having read arctile 2-13 I think the first article is the most important for me. If I do something now that’s going to be illegal later, I will have an advantage over the new law.

**Read about (cyber) ethics, give a summary of aspects, views and opinions including your own point of view on some of these aspects and views.**

**Know the rules of cyber ethics (short).**

The basic rule is “Do not do something in cyberspace that you would consider wrong or illegal in everyday life.” (know rules cyber ethics, n.d.)

This obviously means stealing, breaking in someone’s computer and cyberbullying are not following the rules of cyber ethics.

**CyberEthics.**

“Cyberethics is the philosophic study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to do, and how this affects individuals and society.“ (Cyberethics, 2019)

The invention of cameras has created a lot of ethical debates. A lot of people really like their privacy, they want to be free from outside intrusion. And even though people like their privacy, they still give a lot of personal information over the internet while making a transaction for example. When I order something from Amazon, they need my home address, email address, bank details, first and last name. that’s already a lot of information of a person. In this case people are willingly giving up their privacy information to a big company.

Because that information is now stored somewhere in a database, it’s possible that it leaks and will then be used by non-ethical hackers.

**Hacker ethic.**

“Hacker ethic is a term for the moral values and philosophy that are common in hacker culture.” (Hacker ethic, 2019)

Hacker ethics believe that sharing information and data is not a bad thing at all. Computers can change people’s lives for the better, and access to computers should be unlimited for everyone. Being able to get all the information you need for free will allow for greater creativity for everyone and any system could benefit from an easy flow of information.

**Difference Between Law and Ethics.**

“In simple terms, the law may be understood as the systematic set of universally accepted rules and regulation. It is used to govern the action and behaviour of people.” (S, 2018)

” Ethics are the principles that guide a person or society, created to decide what is good or bad, right or wrong, in a given situation. It regulates a person’s behaviour or conduct and helps an individual in living a good life, by applying the moral rules and guidelines.” (S, 2018)

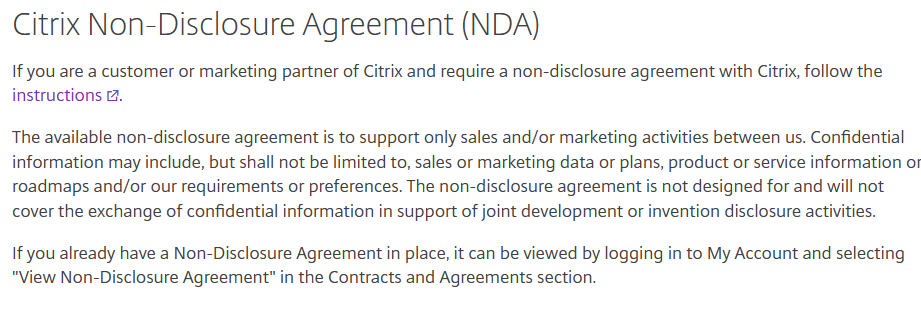
This means that there really is a difference between law and ethics. Law is a set of rules while ethics are more like a set of guidelines. This means that ethics are about the morals of a person and that law is about a prescribed set of rules made by other people. Every person is bound by the laws of a country, it clearly defines what a person can and cannot do.

Knowing this, it’s important to know that the breach of a law may result in punishment which is not the case of an ethical breach.

**Introduce and explain the concept of responsible disclosure and find and compare two or three Responsible Disclosure policies from different companies.**

**Non-disclosure:**

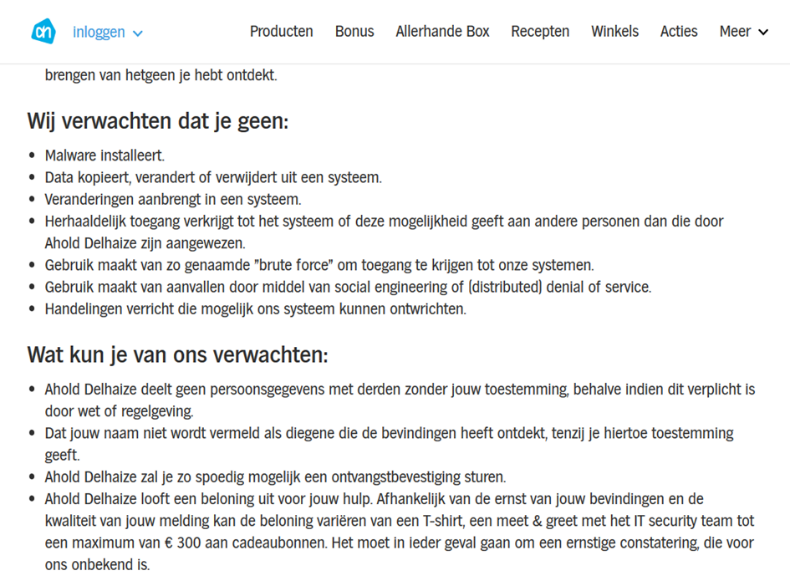
Non-disclosure makes sure that no vulnerability information can be shared or can only be shared under non-disclosure agreement.



(citrix non disclosure agreement, n.d.)

**Responsible disclosure:**

Responsible disclosure is a disclosure in which a vulnerability is disclosed only after some time. This allows the company to patch the vulnerability before it is made public. This period makes a key difference between responsible disclosure from full disclosure.



(meldpunt kwetsbaarheden, n.d.) & (responsible disclosure, n.d.)

Now there is a big difference between these 2. Obviously, the ING has to be way more careful about this than ah. Because of this the responsible disclosure of ING contains way more information than the one from ah. They have, more rules, higher rewards, more information and more things that aren’t allowed.

**Full disclosure:**

Full disclosure publishes software vulnerabilities as fast as possible, making the data accessible to everyone. The purpose of this, is to make the potential victims as knowledgeable as those who attack them.

### Afterthoughts

When I started, I didn’t really know about the disclosures. But this assignment gave me more knowledge about the law and ethics behind hacking. I’m sure I can use this knowledge in my project when performing a pentest for a company.

## 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

### 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. The instruction also didn’t really feel for beginners and was in English/Dutch at the same time.

### 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 person’s 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**: "Foot printing (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.

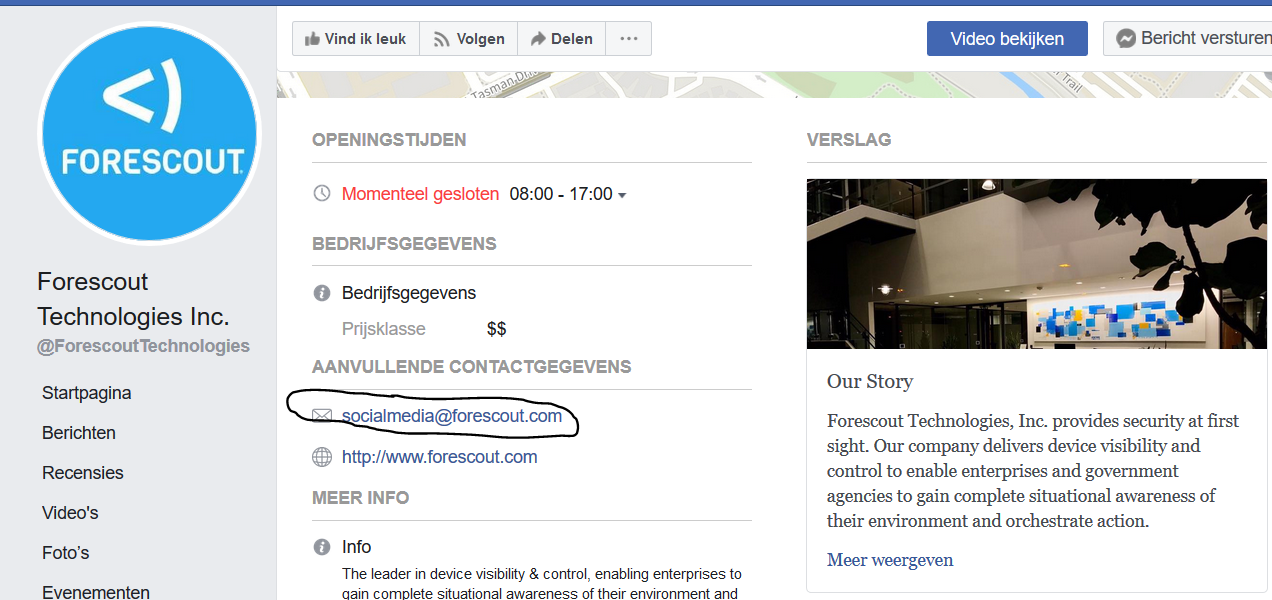
To gain this information the hacker uses different types of tools. But when researching for information the hacker doesn’t have to start with typing some commands in. A simple google search could gain the hacker a lot of information about a company. But after that the hacker would have to use tools like,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

### Execution

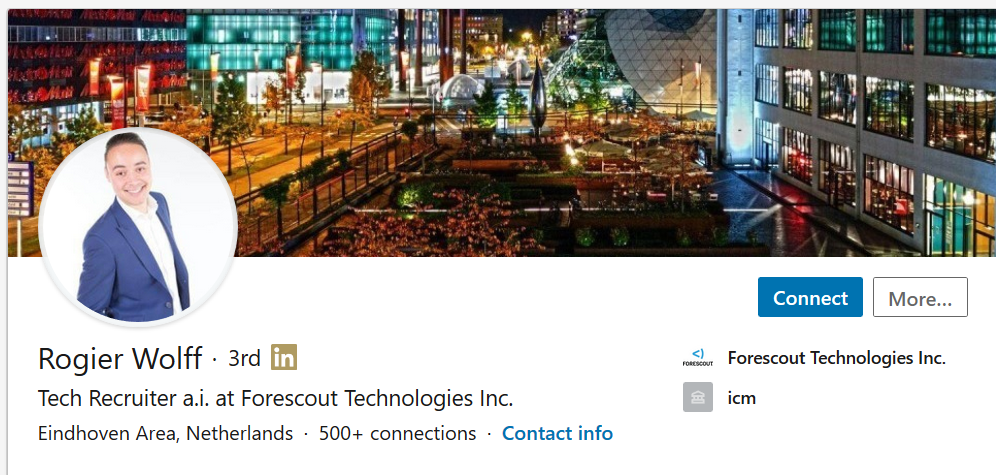
#### Basic challenge

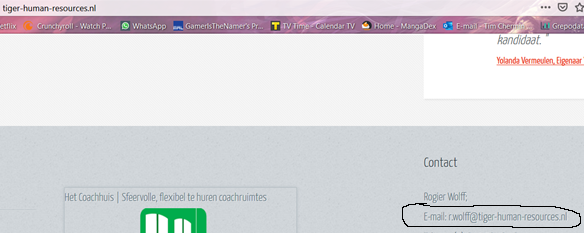
Find at least 3 people including email address (not management) which work with secmatters.com using social networks like LinkedIn.

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

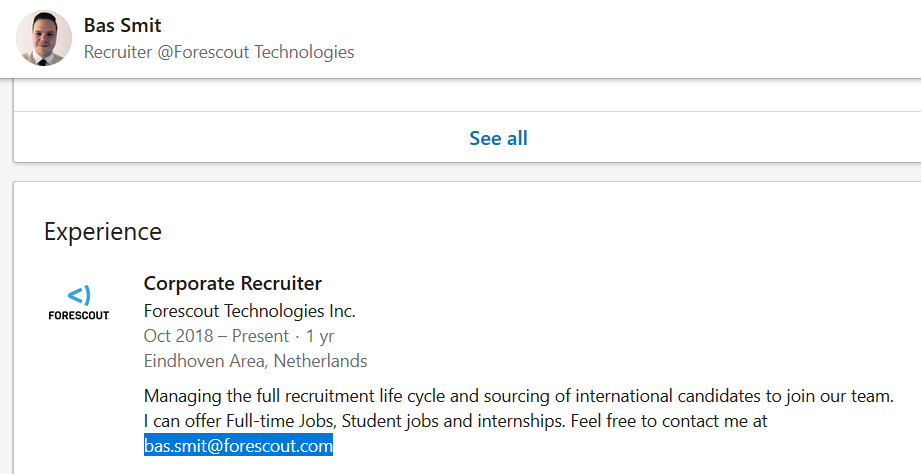


After doing some research I found a mail address on the website of an employee through his twitter.





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



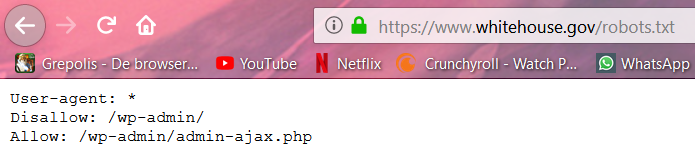
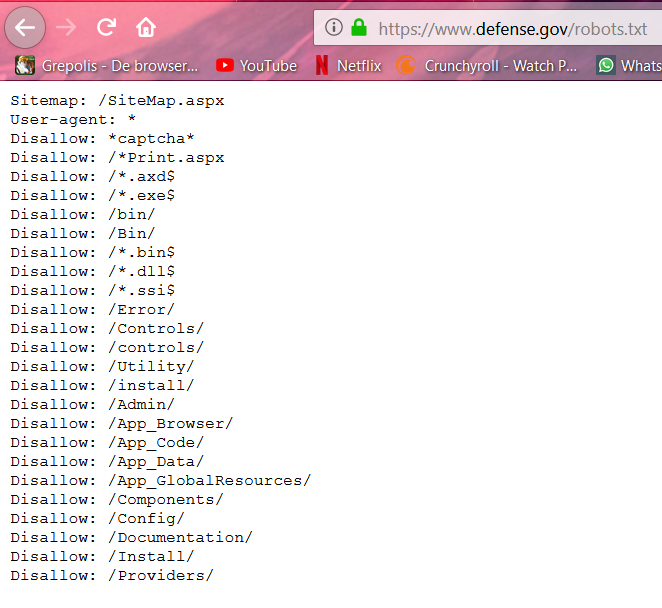
**Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org.**



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).

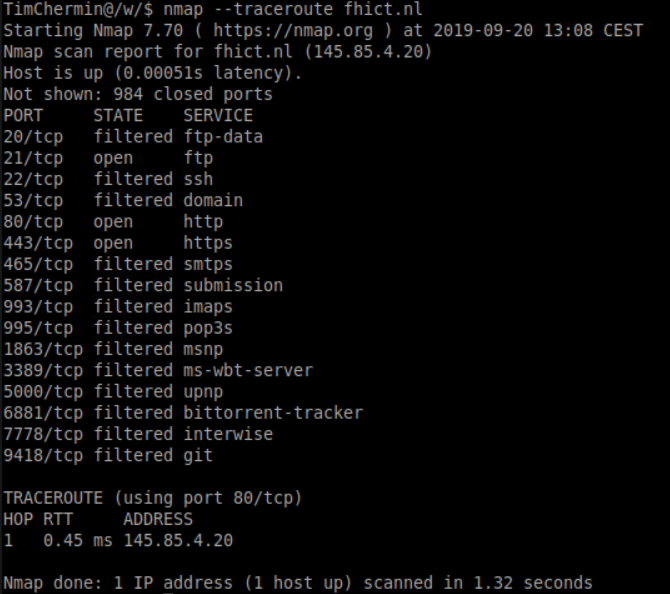
**Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.**

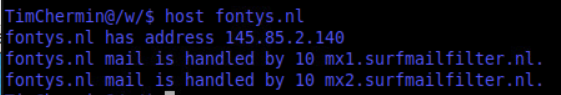
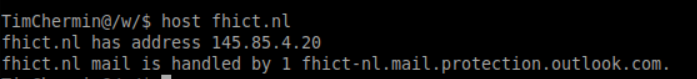
At first, I had no idea what robot.txt was but after a quick google search I found these results. “Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called The Robots Exclusion Protocol.” (robotstxt, n.d.)



**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.)

**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 foot printing part of this subject. But the challenges helped me understand it a bit more. And again, the instruction was pretty much useless for me.

## 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:**

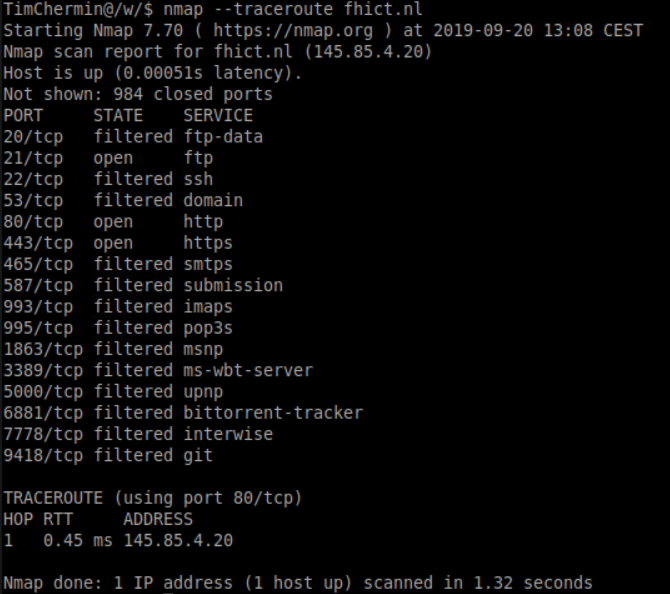
Nmap is a free open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, Ip address detection and operating system detection.

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
* Registered ports 1023-49151
* Dynamic ports 49152-65535 used on client side

For example, FTP has 21 and http has 80. In the image bellow you can see the different ports when using the nmap –-tracerout fhict.nl command.



There are 6 different states that ports can have:

* Open: actively accepting TCP, UDP or SCTP associations on this port. (hackers want to find these)
* Filtered: nmap can’t determine if it’s open or not because of packet filtering.
* Closed: accessible, but there is no application listening on it.
* Unfiltered: accessible, but nmap can’t determine if it’s open or closed.
* Open|filtered: nmap can’t determine if it’s open or filtered.
* Closed|filtered: nmap can’t determine if it’s closed or filtered.

**TCP:**

TCP (Transmission Control Protocol) is one of the main protocols of the internet. TCP provides reliable and error checked delivery of a stream of bytes between applications running on hosts that communicate via an IP network.

**UDP:**

Applications that don’t require the reliable data stream of TCP, may use the UDP (User Datagram Protocol). UDP provides a connectionless datagram service that emphasizes reduced latency over reliability

**A few of the different type of scans**:

-sS (TCP SYN scan): SYN scan is the default option. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. (nmap, n.d.)

-sT (TCP connect scan): TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. (nmap, n.d.)

-sU (UDP scans): UDP scan works by sending a UDP packet to every targeted port. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, but for most ports the packet is empty unless the --data, --data-string, or --data-length options are specified. If an ICMP port unreachable error (type 3, code 3) is returned, the port is closed. Other ICMP unreachable errors (type 3, codes 0, 1, 2, 9, 10, or 13) mark the port as filtered. (nmap, n.d.)

**Network enumeration** is an activity in which usernames and info on groups, shares, and services of networked computers are retrieved. Network enumeration is the discovery of hosts or devices on a network. Network enumeration tends to use overt discovery protocols such as ICMP and SNMP to gather information. It may also scan various ports on remote hosts for looking for well-known services to further identify the function of a remote host. The next stage of enumeration is to fingerprint the operating system of the remote host. (network enumeration, n.d.)

**Scanning anonymously:** 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.

### Afterthoughts

When I started, I already did some scans because of another subject so it helped with understanding this one more. I think I wasted too much time on this since it’s hard to find a point to stop doing research. And again, the instruction was pretty much useless for me.

## 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

### Relevance

When a database is vulnerable for SQL injections it could be dangerous for a company. When a database contains valuable information like, passwords, emails, phone numbers and addresses. They could be used by black hat hackers to steal money or information.

### Starting point

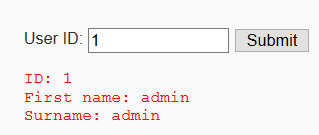
I didn’t know anything about SQL-injection before this assignment.

### 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.

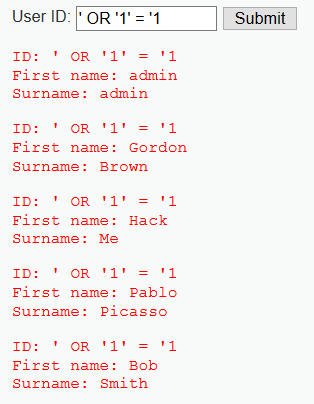
### Background information

### Execution

**DVWA challenge**

I started with just trying to give a user ID and seeing if I will get a result to start with.

And I found this after some time.

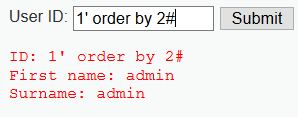


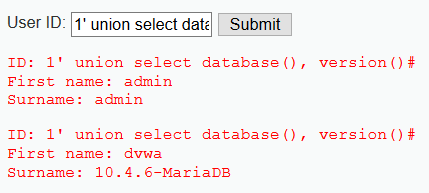
After following the instruction I got this clause. This will change the WHERE …. IS … with ’ OR ‘1’ = ‘1 because 1=1 is always true it will give all the users.



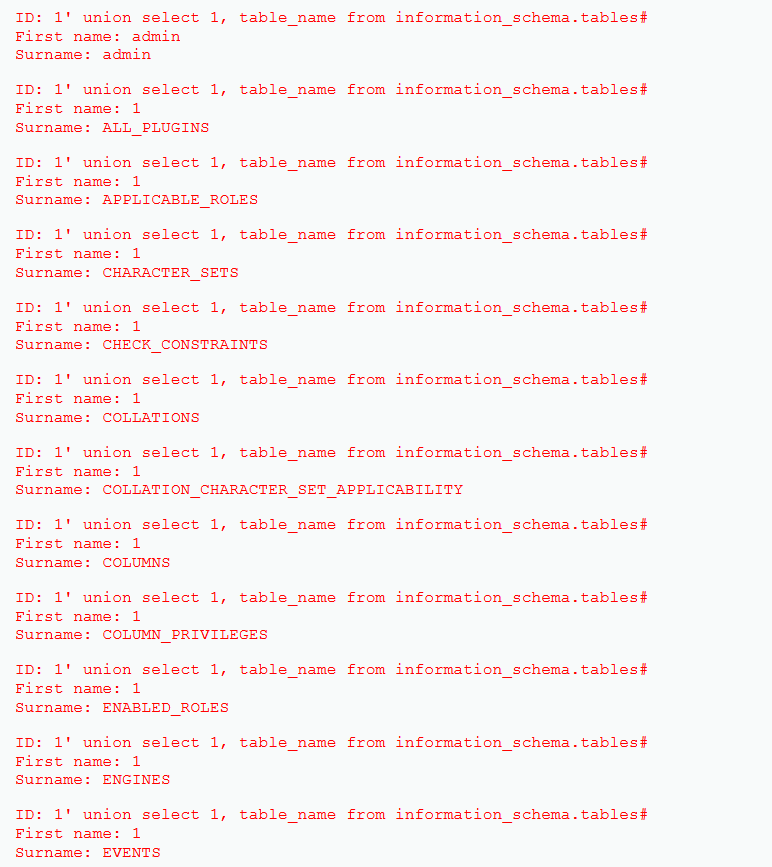
Using 1’order by 3# you get an error this means that there less than 3 columns



Using 1’order by2# I found out there are 2 columns. I will also be using this information for the next clause.

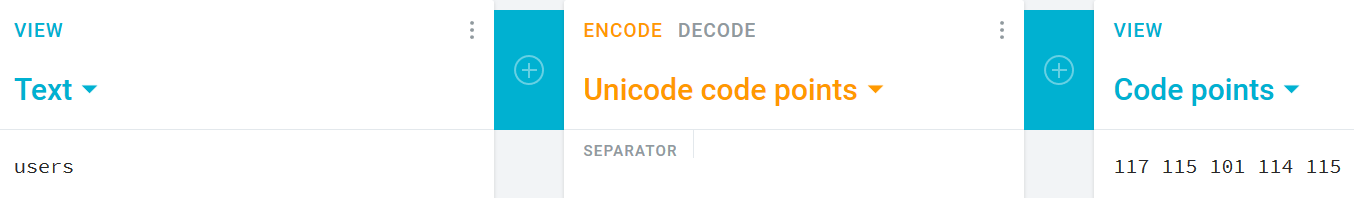
 The UNION operator is used to combine the results of two or more SELECT statements.

So when adding select database(), version()# it will give the database name as first name and the version of the database as the surname. # in MySQL is used for a comment so it will ignore everything after version().

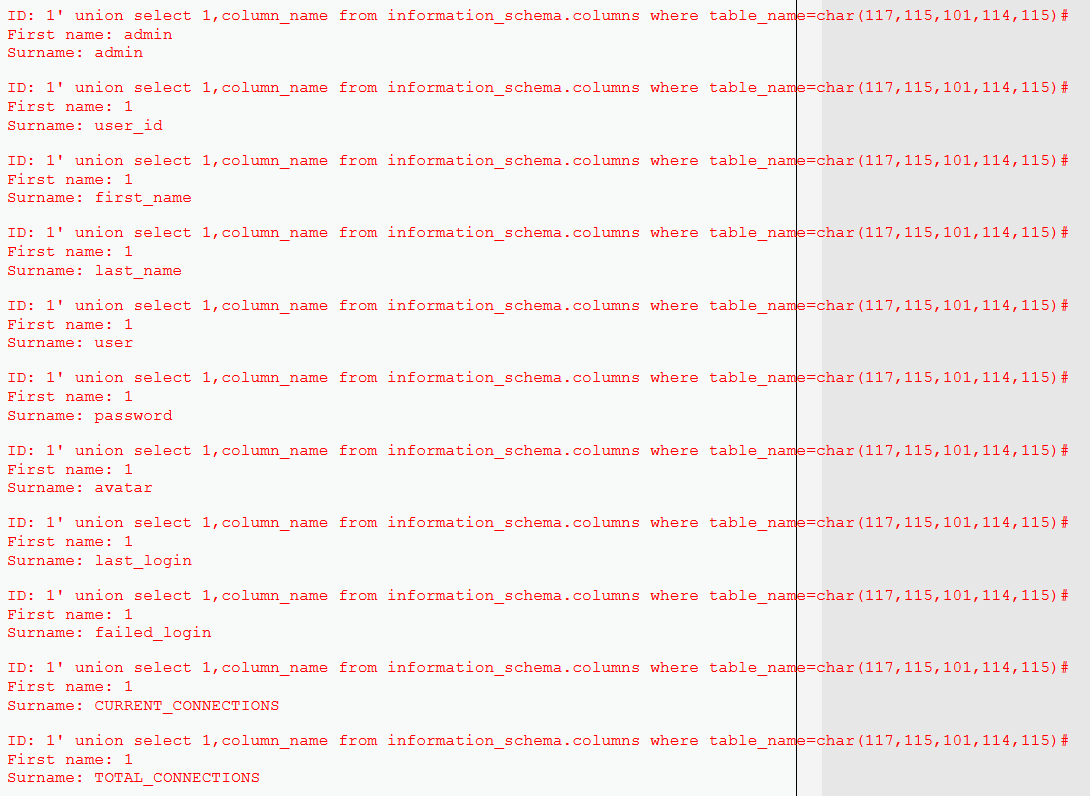
Using

1' union select 1, table\_name from information\_schema.tables#

Since I only wanted to look at the table names I kept the first name as 1. As the surname I wanted to look at the table names in the database using table\_name from information\_schema.tables.



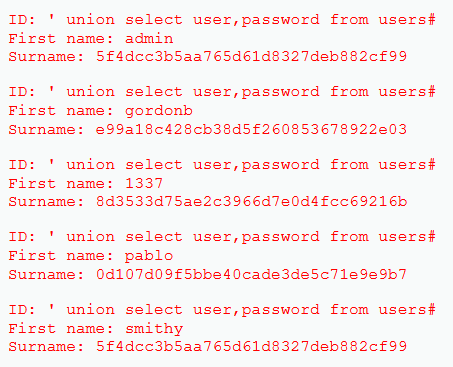
<https://cryptii.com/pipes/text-decimal>



1' union select 1,column\_name from information\_schema.columns where table\_name=char(117,115,101,114,115)#

This will get all the columns with the name in a given table. Using the decimal equivalent in the char function instead of users.

In the columns of the users there is a column called password. This can be used to find the passwords of the users.



' union select user,password from users#

This will speak for itself



Using <https://crackstation.net/> the passwords were easily cracked.

<https://www.youtube.com/watch?v=GLvrieLufTA>

### Afterthoughts

Looking back, I learned the basics of SQL injection with the help of a YouTube video. This knowledge will hopefully help me in the future. What I tried is not to just copy the video, but to understand and maybe even change the inputs.

## 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)

### Relevance

The tools are needed for almost all of the subjects.

### Starting point

I had never heard of any of these tools before.

### Approach

I started with following the instruction about this subject and after the instruction I tried the basic challenge.

### Execution

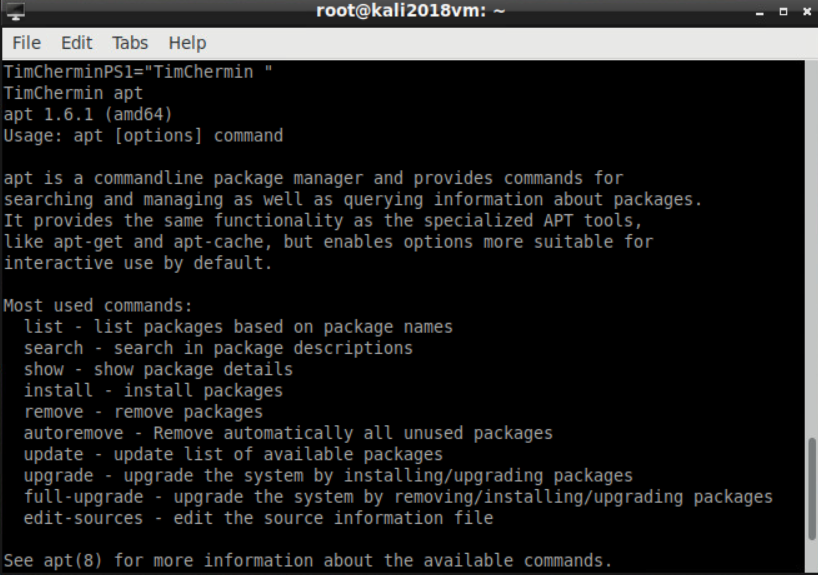
#### Linux basic skills

Using the Linux command overview on canvas I started with looking at the basics of the basics before I was going to start the ‘overthewire’ challenge.

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

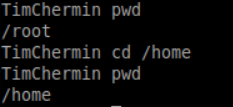
**Command line activities:**

**APT:**



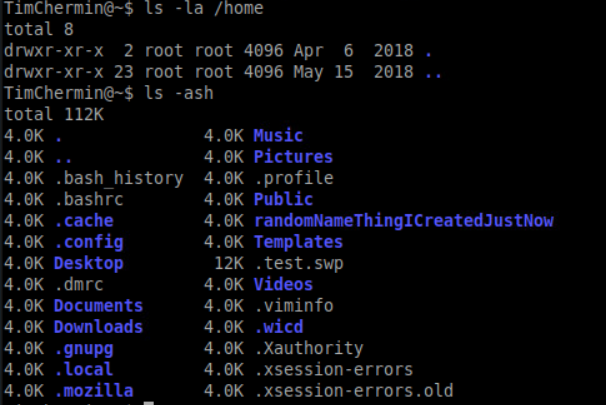
The CLI's apt command lets you search for, install, and remove software and add new repositories.

**Pwd:**

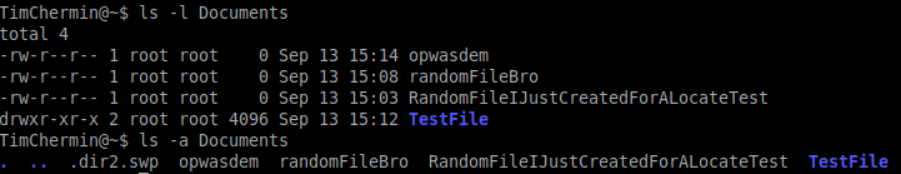


Use the pwd command to print the working directory (the current directory you are in).

**ls -la /home**

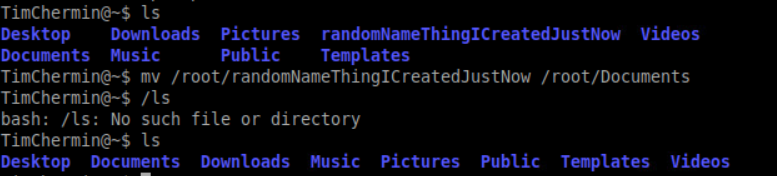


Lists ALL the files and directories in the /home directory, in the long listing format.

**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.

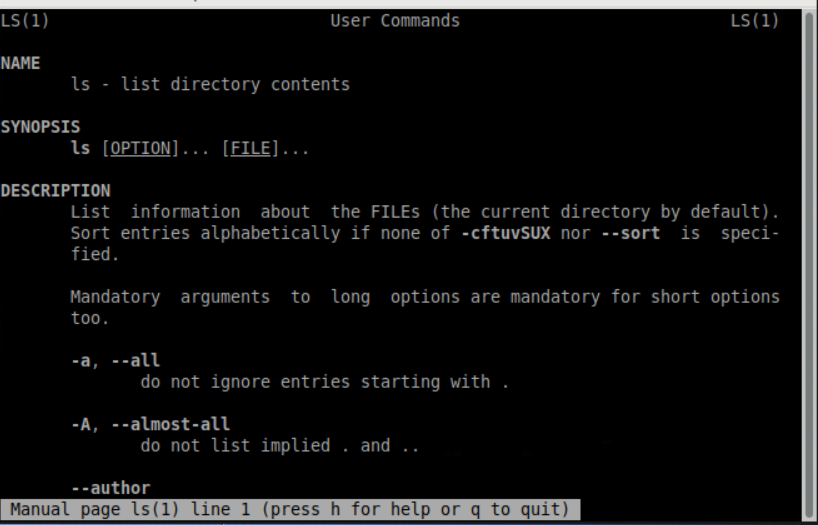
**Mv:**



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

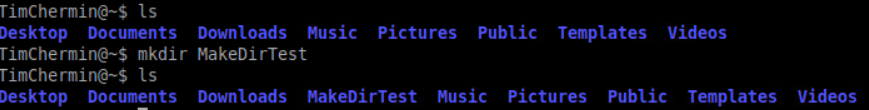
**Man:**

**Man ls:**

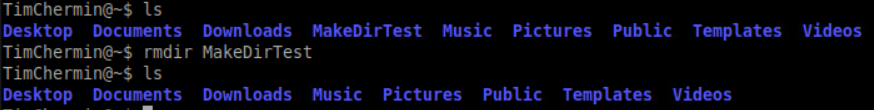


The manual command shows the manual of the inputted command.

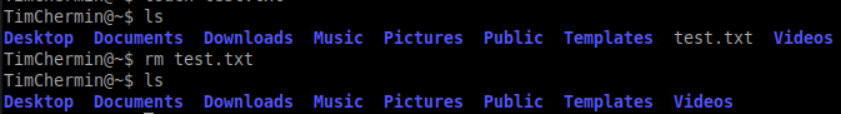
**Mkdir & rmdir & rm:**



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.

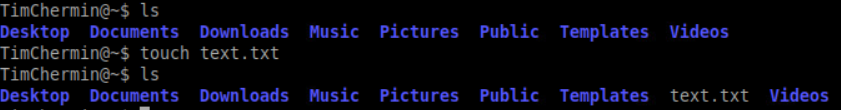


The rmdir(remove directory) command allows the user to remove an existing empty directory.



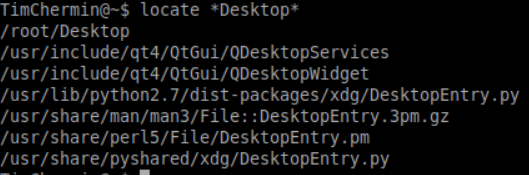
The rm command will remove directories and files held within, the rm command will delete created files.

**Touch:**



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

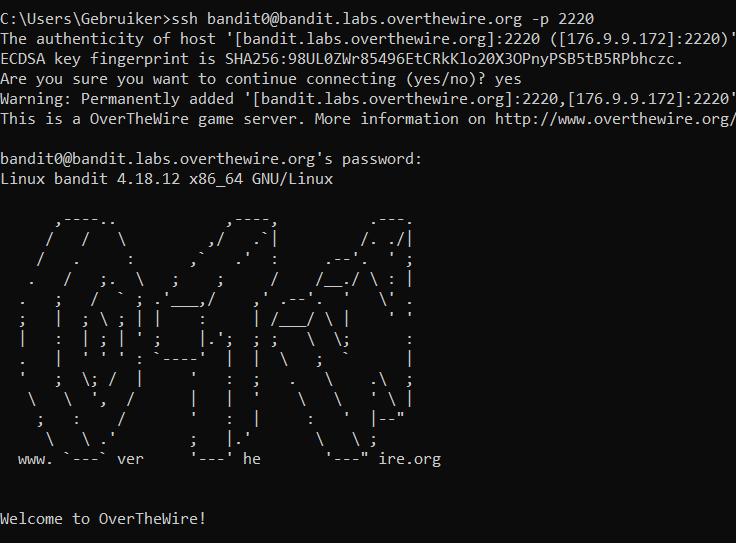
**Locate:**



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

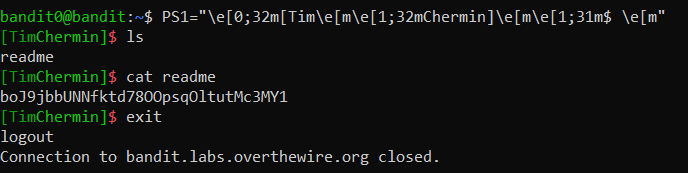
**Overthewire challenge:**

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

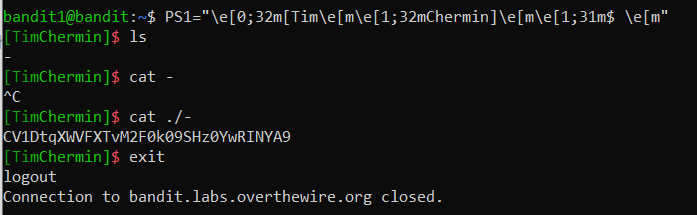


Every lvl the game gives a list of useful commands for that lvl. Using the ‘man’ command I can look into the useful commands to complete the lvl. When I use a quote in this part it means I couldn’t find the info I needed using man so I had to search on the internet for possible commands to use.

**0 --> 1**

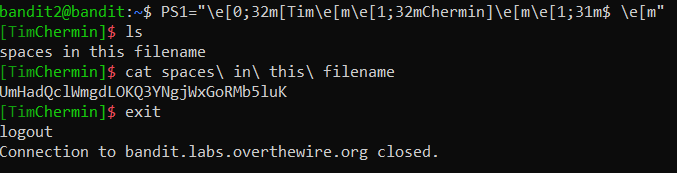


**1 --> 2**



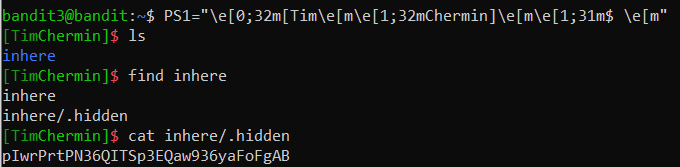
(camh, 2011)

**2 --> 3**



(scarecrow, 2013)

**3 --> 4**

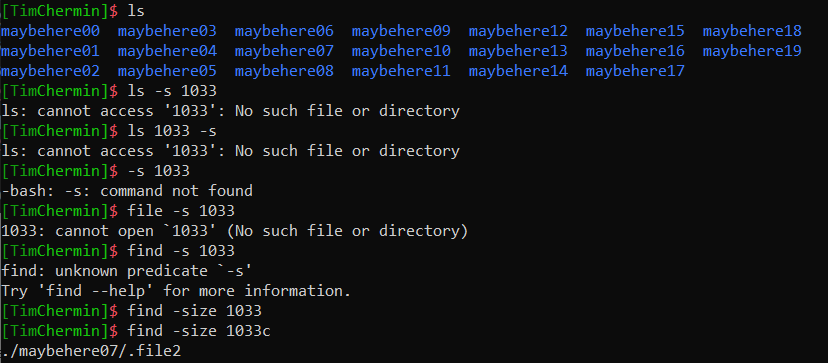


**4 --> 5**

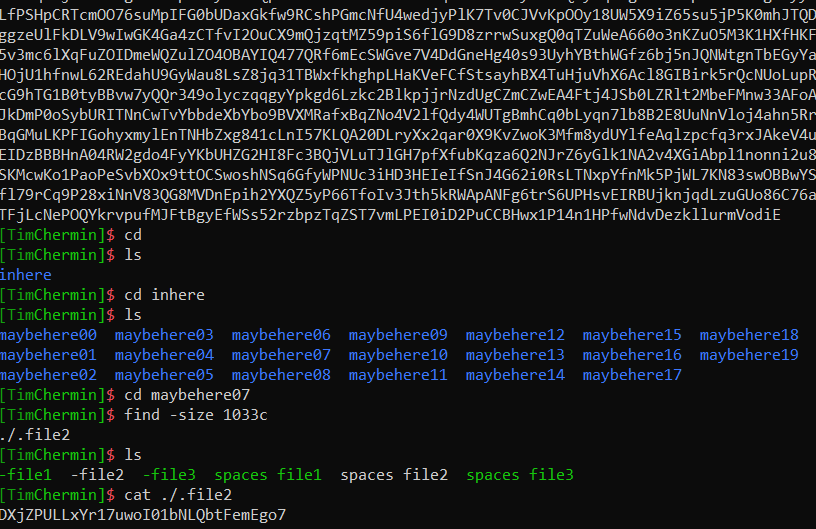


**5 --> 6**

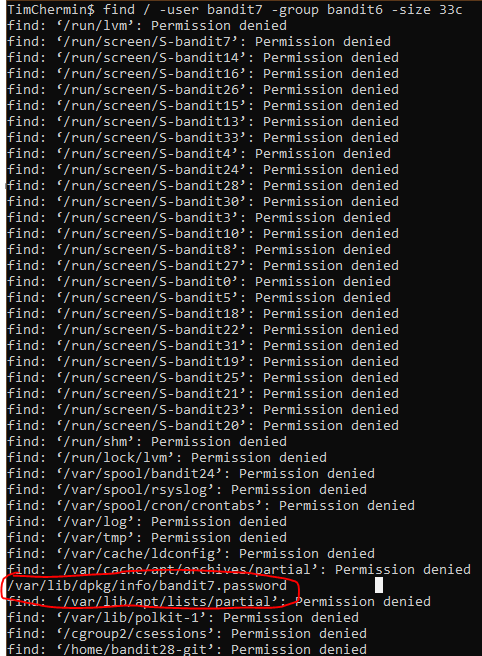
“Find -readable” gave to many results to use.



(Ducea, 2008)



**6 --> 7**





(how do i find all the files owned by a particular user or group, 2018)

I couldn’t really figure this out on my own, so I had to use google to look for possible options for me to use.

**7 --> 8**



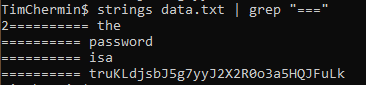
Using man grep first helped me figure this lvl out pretty fast but..after a lot of tries I found out I was spelling millionth wrong…. (I spelled it as milionth)

**8 --> 9**



(pipes, n.d.)

**9 --> 10**



(pipes, n.d.)

**10 --> 11**



By just using man base64 I got this answer quick.

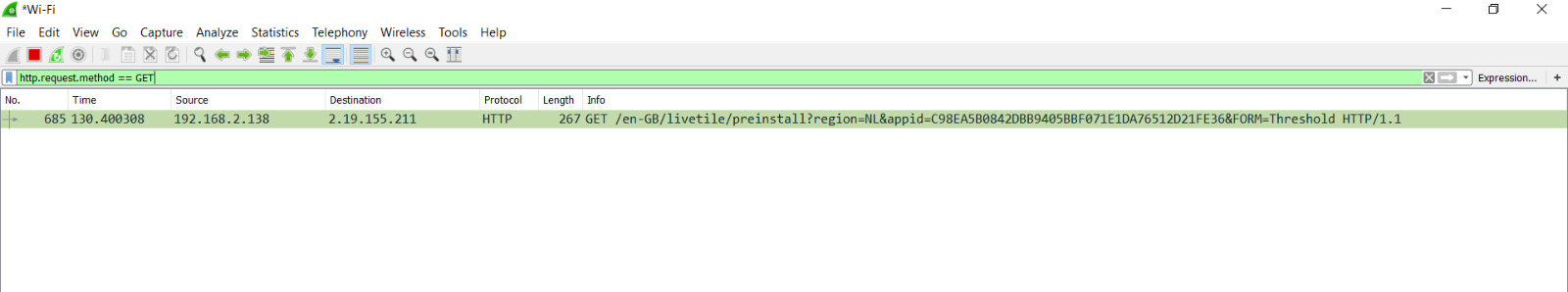
##### Afterthoughts linux

I think I handled Linux as one of the best subjects I have done until now. I started with some basic research and after some time I decided I was ready for the ‘overthewire’ challenge. I really feel like I learned a lot from the challenge.

#### Wireshark

**Challenges:**

**Using display filters to find and see what you want to see in your capture:**



**Basic**:

* [basic use of wireshark (Links to an external site.)](https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/) en/of via [youtube-uitleg (Links to an external site.)](https://www.youtube.com/playlist?list=PL6gx4Cwl9DGBI2ZFuyZOl5Q7sptR7PwYN):   
  sniffing packets and viewing packet details on ip-layer, tcp-layer, and application layer (e.g. Http)
* using wireshark during your hacking and pen-testing:  
  - Show what a portscan looks like with wireshark (Syn-scan, connect-scan, XMAS-scan, etc.) in the module [Network Scanning and Enumeration](https://fhict.instructure.com/courses/8790/pages/network-scanning-and-enumeration)  
  - Show what a MitM Arp-spoofing attack looks like with wireshark in the module [Network Sniffing and Spoofing](https://fhict.instructure.com/courses/8790/pages/network-sniffing-and-spoofing).  
  - Show confidential or personal data when networksniffing with wireshark in the module [Network Sniffing and Spoofing](https://fhict.instructure.com/courses/8790/pages/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)

# 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

camh. (2011, July 9). *usage of dash in place of a filename*. Retrieved from stackexchange: https://unix.stackexchange.com/questions/16357/usage-of-dash-in-place-of-a-filename

Ducea, M. (2008, February 12). *linux tips find all files of a particular size*. Retrieved from ducea: http://www.ducea.com/2008/02/12/linux-tips-find-all-files-of-a-particular-size/

*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

*how do i find all the files owned by a particular user or group*. (2018, September 5). Retrieved from cyberciti: https://www.cyberciti.biz/faq/how-do-i-find-all-the-files-owned-by-a-particular-user-or-group/

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

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

*network enumeration*. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Network\_enumeration

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

nmap. (n.d.). *port scanning techniques*. Retrieved from nmap: https://nmap.org/book/man-port-scanning-techniques.html

*pipes*. (n.d.). Retrieved from westwind: http://www.westwind.com/reference/os-x/commandline/pipes.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

scarecrow. (2013, June 12). *cannot cat file wich has space in name in linux*. Retrieved from superuser: https://superuser.com/questions/606874/cannot-cat-file-which-has-space-in-name-in-linux/606878

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

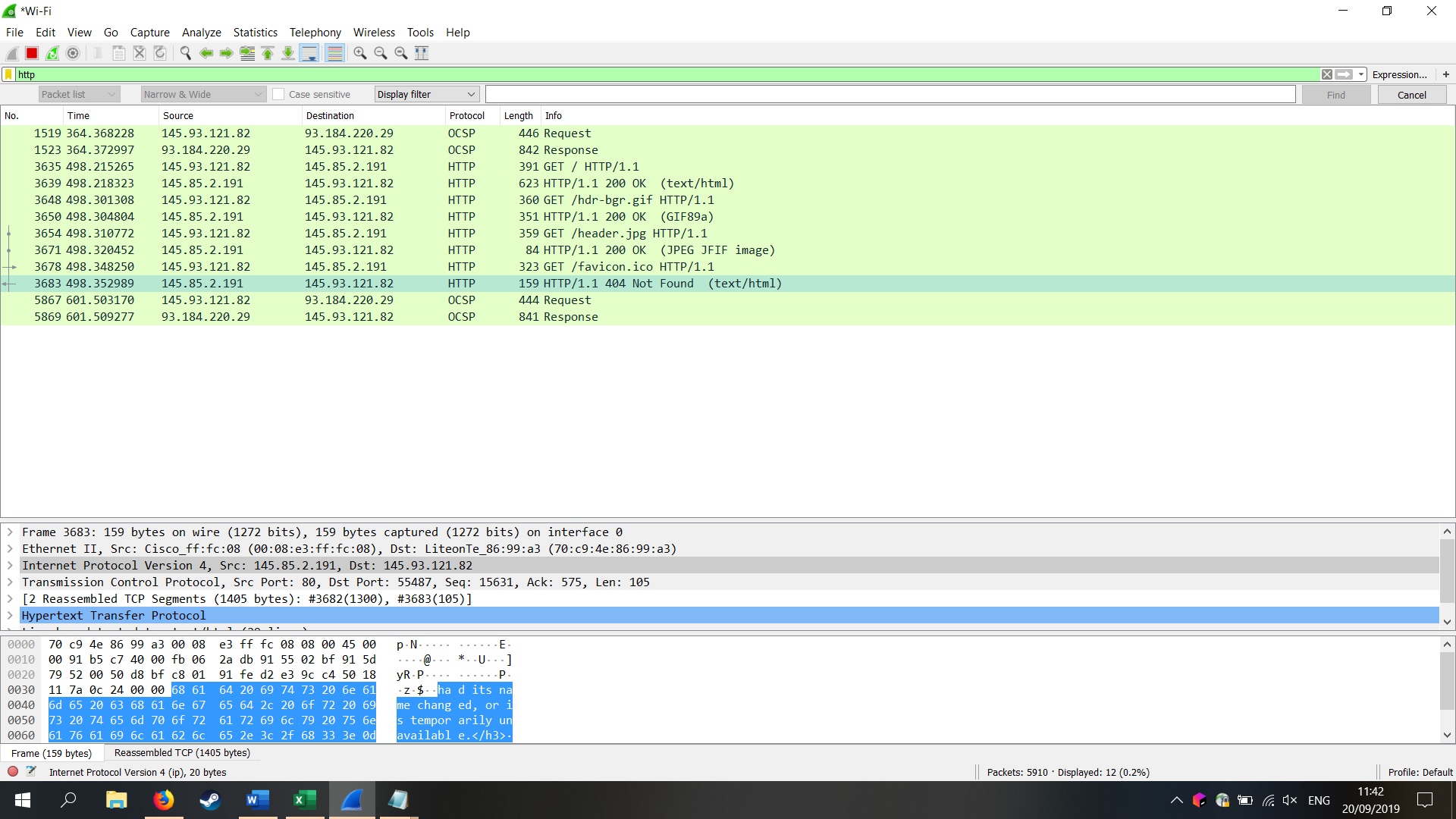
* A(Address) maps a hostname to an IP address
* SOA (start of authority) identifies the DNS server responsible for the domain info
* CNAME (canonical name) provides additional names or aliases for athe address record
* MX(Mail exchange) identifies the mail server for the domain
* SRV(service) identifies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

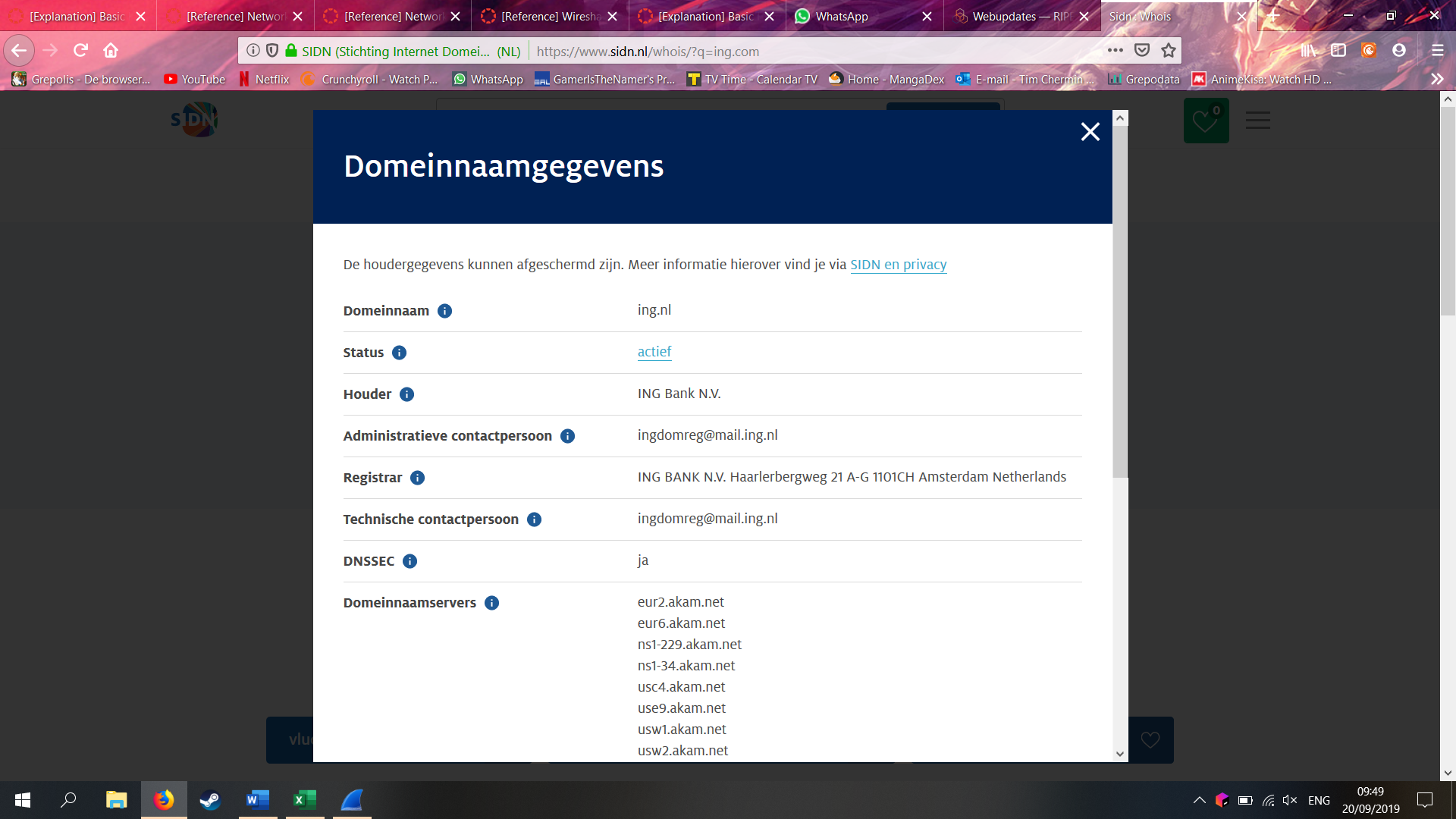
Http-filter <http://merlijnw.freaze.eu/>



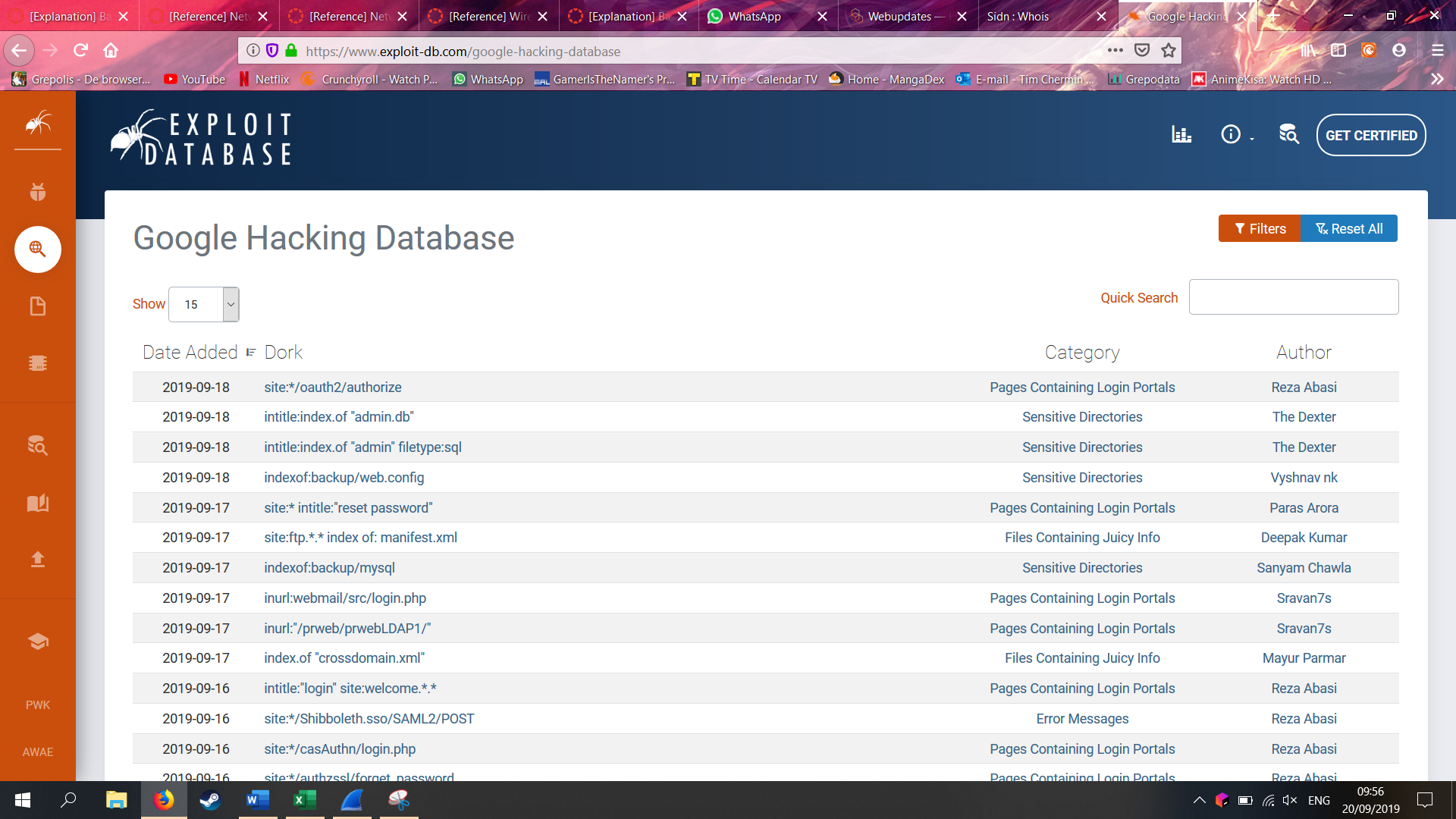
<https://www.shodan.io/>

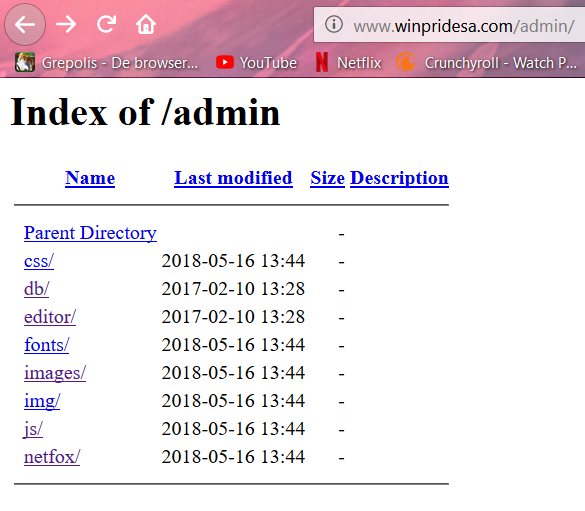
<https://www.ripe.net/>





**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> 



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.