# **Portfolio**

#### Student: Le An

#### Student number:3466604

# Table of contents

# Introduction

# Law, Ethics and Responsible disclosure

# Basic hacking process

### 1.Linux skill

### 2.Wireshark

### 3.Basic Hacking and Pentesting Process

### 4. Law. Ethics and Responsible Disclosure

### 5.Footprinting ,Reconnaissance and Social Engineering

### 6. Network Scanning and Enumeration

## **Introduction**

This document is to show how I understand basic knowledge of hacking, networking through the way I explain and apply it. Besides, I would like to point out the advantage and disadvantage of this course( what’s good or bad).

The 'basic knowledge' portfolio part of this semester is to learn about knowledge of IT Security that helps me improve my technical skills. For me, hacking is a new aspect and it also really interesting.

For the basic knowledge assignment, I will prove knowledge of the following subjects:

- Law, Ethics and Responsible Disclosure

- Basic Hacking Process

- Social Engineering and Foot printing

- Network Scanning and Enumeration

- Network Sniffing and Spoofing

- SQL Injection

- XSS Cross Site Scripting

- CSRF

- Path Traversal

- Password Cracking

- Wireless hacking

- Tooling Linux, Kali, Wireshark, Web Proxies

- Buffer Overflows

## **II. Law, Ethics and Responsible Disclosure**

Nowadays, More and more hackers are attacking information systems around the world, threatening the information of millions of internet users. This makes the issue of law and ethics more and more noticeable. Besides the law which is created by the government to govern the entire society and actions of each member, ethic is something which is similar to the law but mostly depends on each individual's moral. Ethics is a branch of moral philosophy that guilds people about basic human behavior like what you are taught to behave in real life such as “Do not take what does not belong to you”. We should put all these things into consideration:

*Do not use rude or offensive language*.

*Do not cyberbully.*

*Do not plagiarize.*

*Do not break into someone else's computer.*

*Do not use someone else's password.*

*Do not attempt to infect or in any way try to make someone else's computer unusable.*

*Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.*

In my point of views, the moral issue cannot be applied to inanimate objects. It can be said that the Internet is just a collection of technical devices linked together through information channels. In other words, the Internet is an inanimate object. That is the mistake that some people often make. They think that they are only interacting with machines, when in fact they have been interacting with humans. Moreover, they also affect sensitive areas of human possession, such as communications secrets, personal secrets. So, these things effects strongly to the internet, it is time to reconsider using purely technical administrators to control the Internet. Need to provide administrators with information systems, a relative amount of knowledge about social sciences and humanities. At the same time, some issues in network management need to be left to law, economist, psychologist and other non-technical experts. However, I have not yet identified which is easier to do - provide social sciences and humanities knowledge training for administrators, or provide technical instruction on the Internet to non-technical human resources.

But for myself, I always remember 4 rules in my mind that helps me avoid causing troubles:

*Do not distribute dangerous information*

*Avoid harmful things*

*Use moderately*

*Always keep it a secret*

* Responsible Disclosure:

According to Wikipedia, responsible disclosure is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mended. This period distinguishes the model from full disclosure. For example, my team is doing implement development practice and suddenly discover a vulnerability, it’s important to clarify a process that allows them to safely report the issue to your team. This is referred to as a responsible disclosure policy.

* Compare to my country’s Law(Vietnam):

## **citing some typical ideas of cybersecurity laws( unofficial English translation)**:

*State policies on network security*

*1. Prioritizing the protection of network security in national defense and security, socio-economic development, science, technology and foreign affairs.*

*2. Building a healthy cyberspace, without prejudice to national security, social order and safety, legitimate rights and interests of agencies, organizations and individuals.*

*3. Prioritizing the resources to build specialized forces to protect network security; capacity building for network security guards and organizations and individuals involved in protecting network security; prioritize investment in scientific and technological research and development to protect network security.*

*4. To encourage and create conditions for organizations and individuals to participate in protecting network security and handling threats to cyber security; research, develop technology, products, services and applications to protect network security; coordinate with functional agencies in protecting network security.*

*5. Enhancing international cooperation on network security.*

*Measures to protect network security*

*1. Measures to protect network security include:*

*a) Assessing network security;*

*b) Assessment of network security conditions;*

*c) Checking network security;*

*d) Monitoring network security;*

*d) Responding and overcoming network security incidents;*

*f) Fight for network security protection;*

*g) Using passwords to protect network information;*

*h) Prevent, request suspension, cessation of providing network information; to suspend and suspend activities of establishing, supplying and using telecommunications networks, Internet, manufacturing and using radio transmitters and receivers in accordance with the law;*

*i) Requesting deletion, access to erase illegal information or false information on cyberspace infringing national security, social order and safety, legitimate rights and interests of agencies, organizations and individuals;*

*k) Collecting electronic data related to activities infringing upon national security, social order and safety, legitimate rights and interests of agencies, organizations and individuals in cyberspace;*

*l) Blockade and restrict operation of information systems; suspend, temporarily suspend or request to cease operation of the information system, withdraw domain names in accordance with law;*

*m) Prosecute, investigate, prosecute, adjudicate in accordance with the Criminal Procedure Code;*

*n) Other measures in accordance with the law on national security and the law on handling of administrative violations.*

As you can see, about my country’s laws, it is similar to international cyber laws, however, there are still lots of vulnerabilities that make it possible for hackers to take advantage of it. My country still tries to enhance the law’s day by day.

## **III. Basic hacking process**

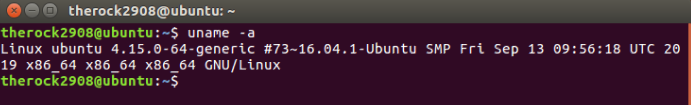
# 1.Linux Skill

From the last semester, I had experiences on Linux, so I decided to go to intermediate level.

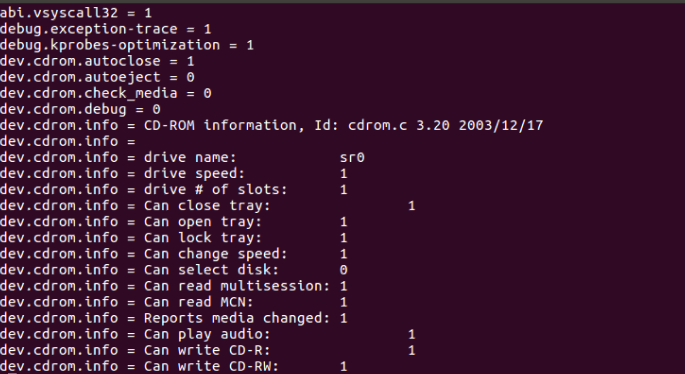
**Linux basic for aspiring hacker 12**

I did all steps following the instruction from website.

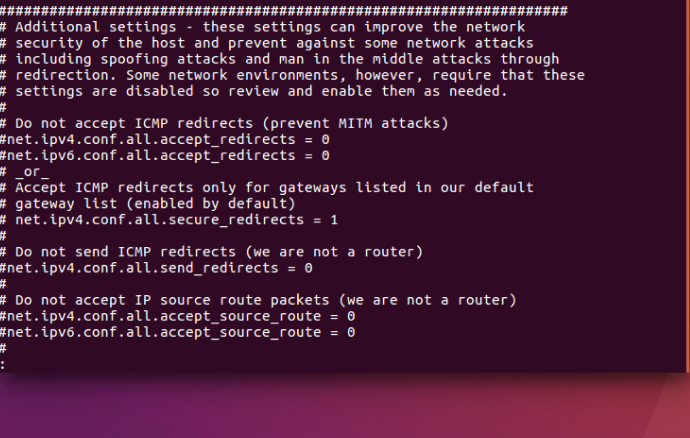
check to see what kernel our system is running



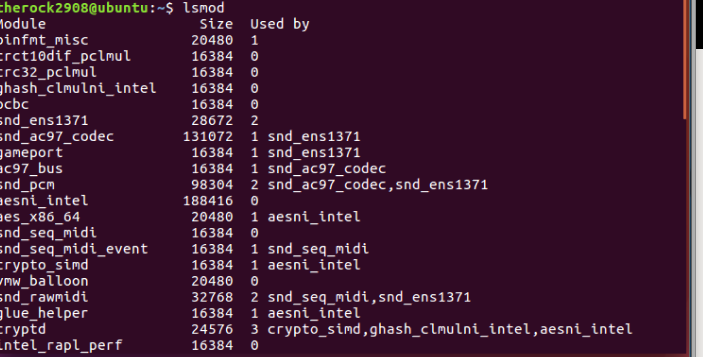
Tune kernel options



View the configuration file for sysctl

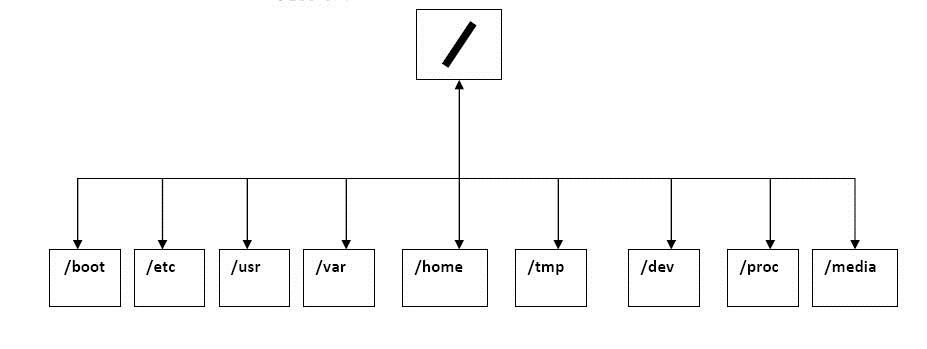


List the installed modules



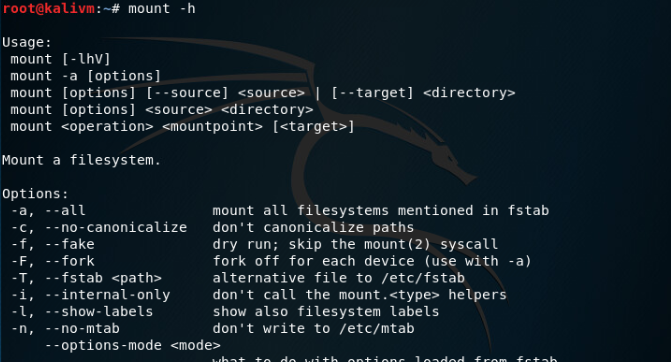
**Linux basic for aspiring hacker 12**

File structure of linux: All the drives and devices are part of single filesystem tree.



Mount Command:

- **mount –h: help screen will display**

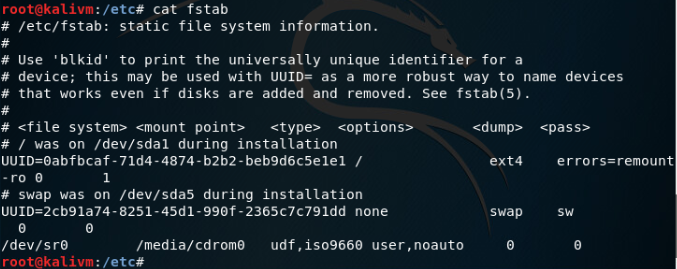


**mount -t filesystemtype location: mount a filesystem of the type (-t) at the location specified. Ex: mount –t /dev/cdrom/media**

**Setting Up Automounting with Fstab**

**Fstab is a system config file in Linux which is read by mount command to determine what options to use when mounting a system.**

**Use command Cat fstab to read stab file:**



**After all, when I want to unmount a drive or divce, I need to use a command Umount:**

**Umount /dev/cdrom: this command will unmount cdrom device.**

**Linux basic for aspiring hacker 16**

In this part, I would like to show about Stdin, Stdout and Stderror which represent where Linux sends the output, where Linux receives inputs and where Linux sends error messages.

Explanation of those commands:

Stdout(Standard Output)(1): Standard output is often referred to as stdout or simply use the numeric representation of 1.

Example: Send Standard Output to a File

Ls /etc/hosts /etc/aircrack-ng 1>anleoutput:   Don't want to see our output messages until after the script has run, but need to see error messages on the screen immediately.

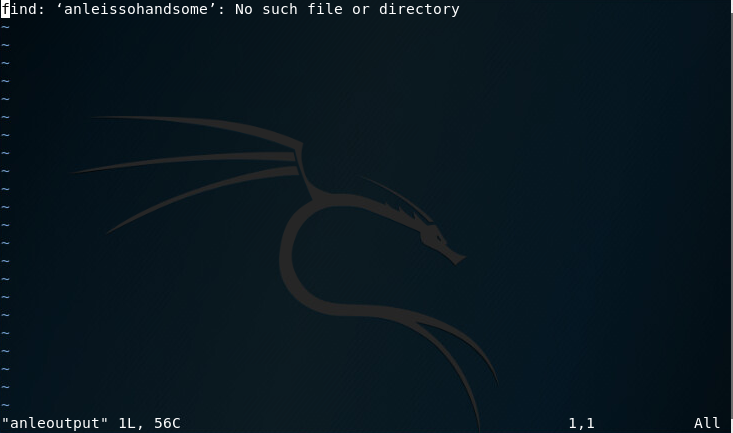


Stdin(Standard Input)(0): Standard input is often referred to as stdin or simply represented by the numeric representation of 0 and it is a stream that represents input into a program (e.g. when a program prompts the user to enter a password)

Stderror(Standard Error)(2): Standard error is often referred to as stderror or simply represented by the numeral 2 and it is another output channel, usually meant for printing debugging information and errors.

Example:

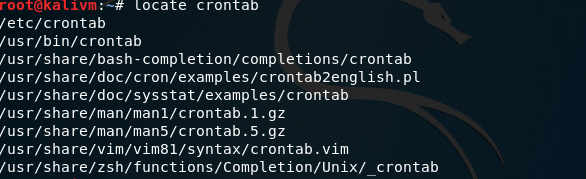




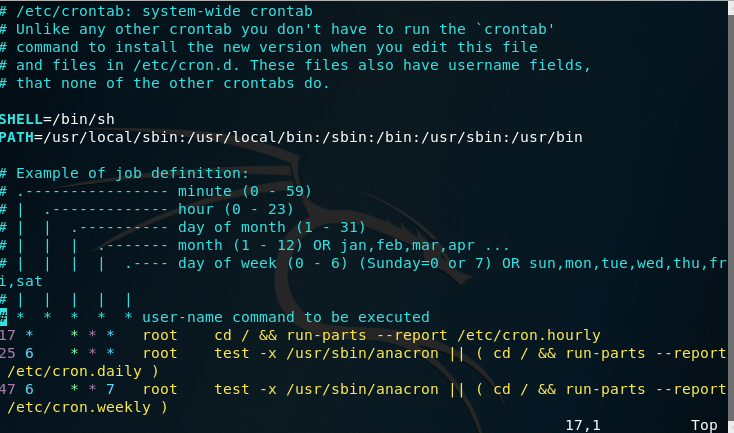
**Linux basic for aspiring hacker 18**

I would like to show you how Cron works in Linux. It typically used to schedule regular tasks such as regular backups at regular times each week.

**Locate crontab**



**vim /etc/crontab : open file crontab**



As you can see on the image, there are some fields:

-minute: the exact minute when the command or job will be run

-hour: the exact hour when the command or job will be run

-day of month: the exact day of the month when the command or job will be run.

-month: the exact month of the month when the command or job will be run.

-day of the week: the exact day of the week when the command or job will be run( 0-6 with Sunday=0).

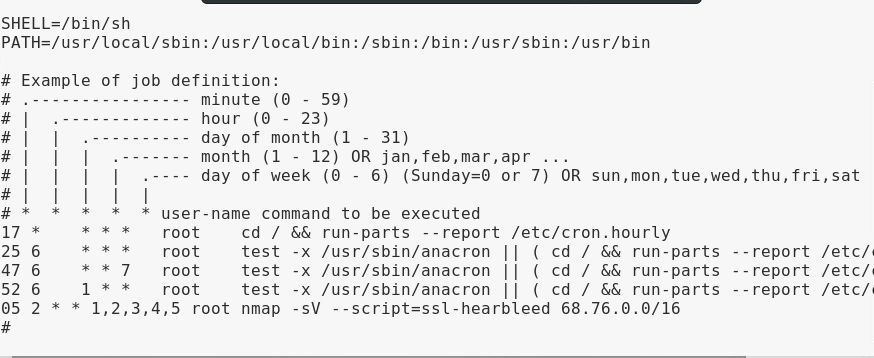
-user: the user permissions that the job will run as

-command: the command I want to run

Furthermore, I also can use Cron to find vulnerable servers such as scanning the globe for IP addresses that are vulnerable. According to the reports, there are about over 300,000 servers are still unpatched that means a lot of vulnerability is still out there.

I will do schedule my heartbleed scanner( exploit the widely disseminated OpenSSL vulnerability that has to become known as "Heartbleed".).

Open file with leafpad and add the text as below. That line of text will schedule nmap hearbleed scanner to run Monday to Friday at 2:05 am for heartbleed vulnerability.



**Bandit lv10-11**

*The password for the next level is stored in the file****data.txt****, which contains base64 encoded data*

*Explain:*

First time, I tried command **base64 filename** but it’s did not work as I expected. After that, I try **base64 –d filename to** decode and it worked.

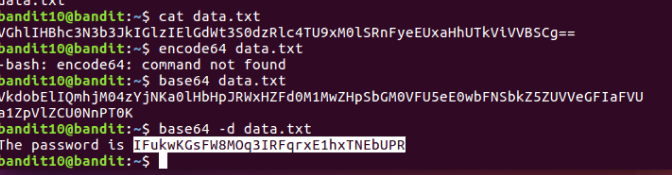
Some basic base-64 commands:

Syntax: **base64 [option] [infile] [outfile]**

Option: **-e(encode)**

-**d(decode)**

-**n(noerrcheck): ignore checking at the time decoding**



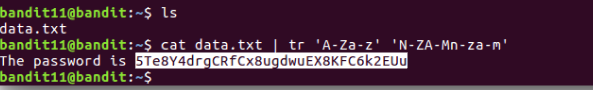
**Bandit lv11-12**

*The password for the next level is stored in the file****data.txt****, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions:*

*Explain:*

According to the article they mentioned below, I found a command to solve this.

**Cat data.txt | tr’A-Za-z’ ‘N-ZA-Mn-za-m’**

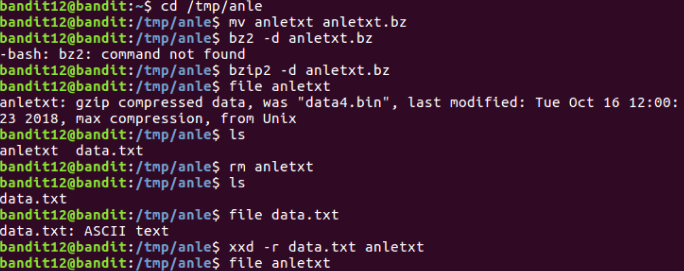


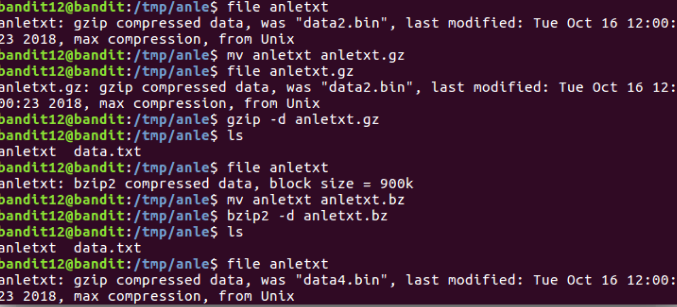
**Bandit lv12-13**

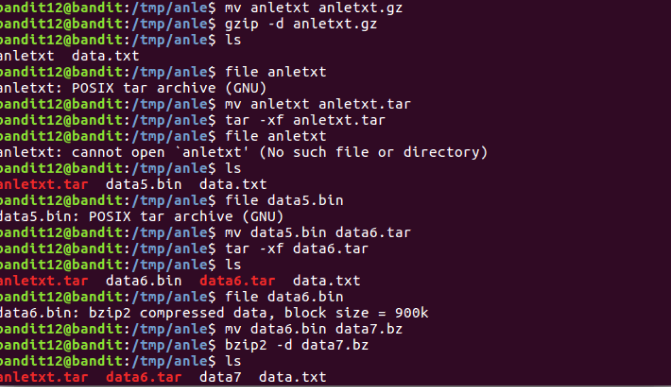
*The password for the next level is stored in the file****data.txt****, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)*

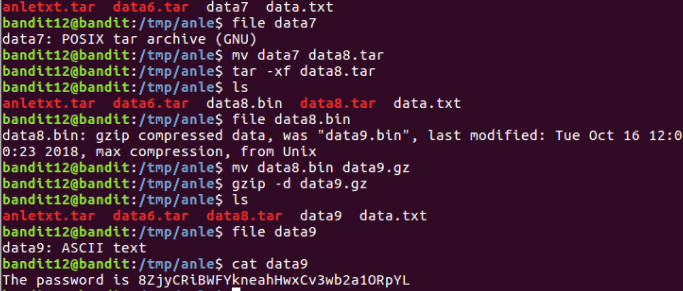
*Explain:*

Firstly, I created a new directory and copy **data.txt** to this directory. I used command: **xxd –r data.txt anletxt** to reverse hex dump data from file and store it in the file with name **anletxt**. Then I used command **file** to check this file and knew that **anletxt** is a gzip compressed file that means I had to use gzip to decompress the file by using command: **mv anletxt anletxt.gz.** After using file command to check information one more time, I used gzip to decompress file and the anletxt.gz was a bzip2 compressed file at that moment. Then, this file became a bzip2 compressed file. Again, I had to change the suffix of **anletxt** to .bz. Then I continued doing same steps until I got file data9 of type ASCII.







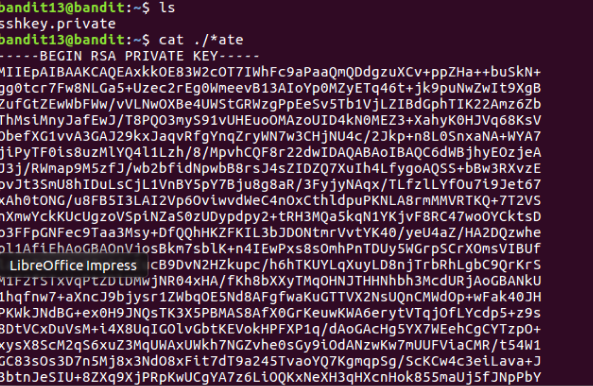


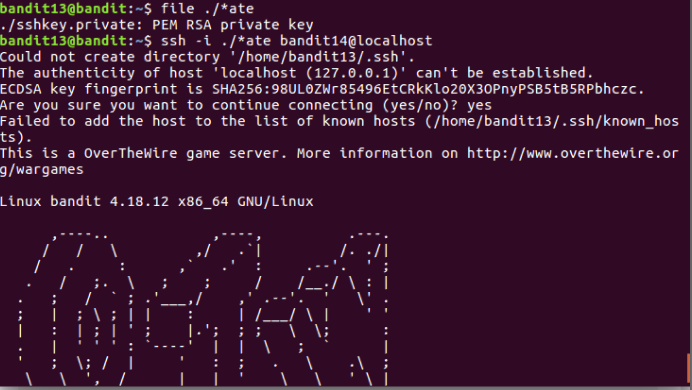
**Bandit level 13-14**

*The password for the next level is stored in****/etc/bandit\_pass/bandit14 and can only be read by user bandit14****. For this level, you don’t get the next password, but you get a private SSH key that can be used to log into the next level.****Note:******localhost****is a hostname that refers to the machine you are working on.*

Explain:

I tried to open this file but it did not show the information I expected then I had to get information from file by using file command then I knew it was a RSA key to open SSH. I searched on google and find a way to open it with command: **ssh –I ./\*ate bandit14@localhost** then it worked.





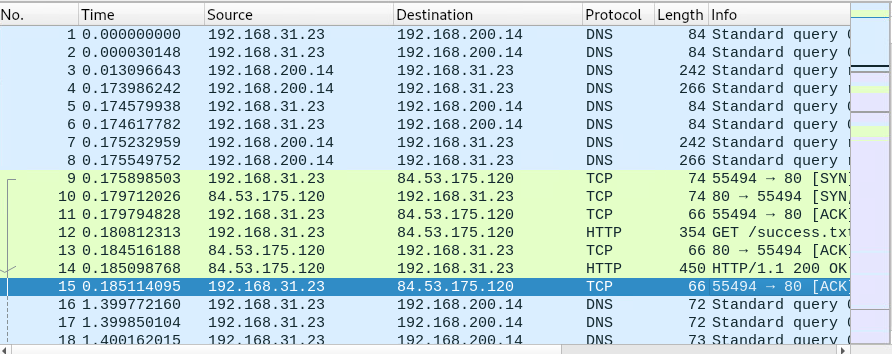
# 2.Wireshark

**What is Wireshark?**

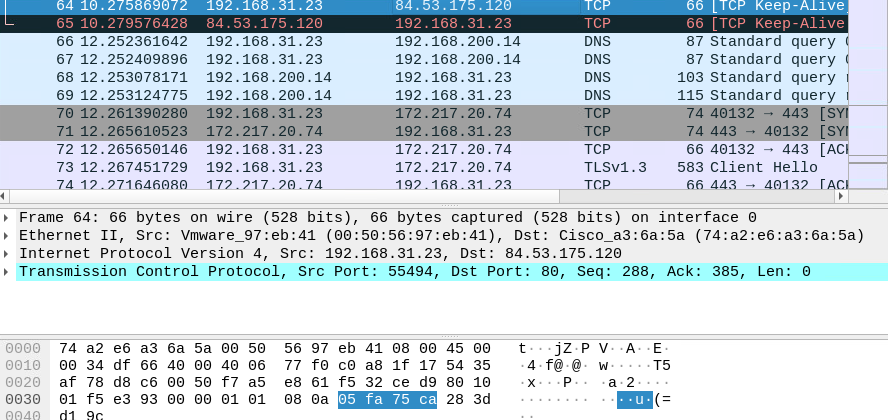
Wireshark is a useful, free analyser which is used for network troubleshooting, analysis, software and communications protocol development. Wireshark was released in 1998 and named Ethereal in beginning of time. Developers used C and C++ to develop whireshark. It is very similar to tcpdump, however, has a graphical font-end with sorting and filtering option. Wireshark lets the user can see all the traffic including unicast traffic.

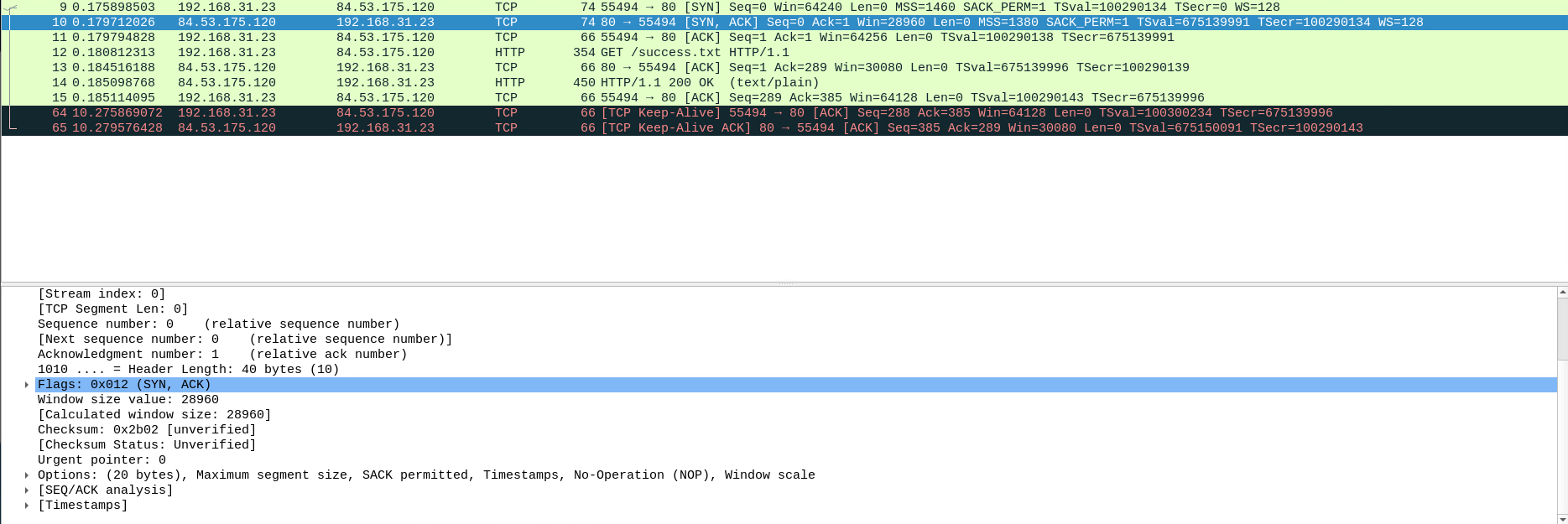
**Basic use of wireshark**

Firstly, after installing Wireshark, I tried to capture the traffic of my network to have an overview of the environment. For me, I chose network interface eth0 and open firefox to see what will happen.



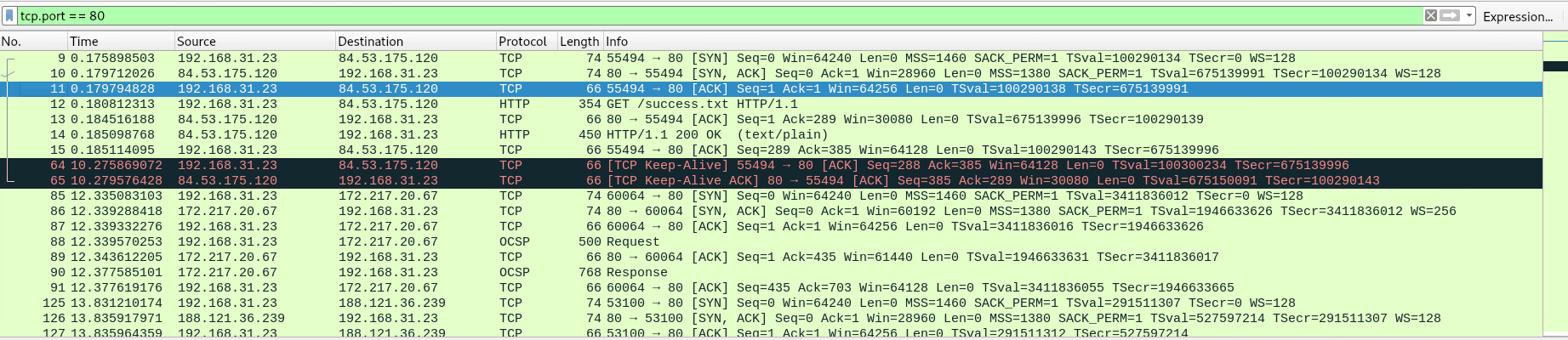
As you can see, all information will be shown on the screen with source IP address( my vm’s address) and destination address as well as protocol**.** Furthermore, I also can click any package on the screen and have more detail.



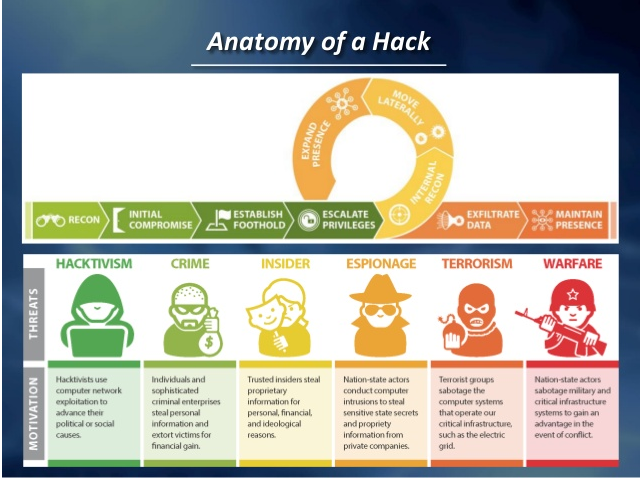


I also can see details of different things such as TCP layer, Http layer



If I want to see only packages go through port 80, I only need filter the traffic that I captured.

# 3.Basic hacking and pen testing process



A good pentest should contain all these standard phases of hacking attack:

Intel gathering: collecting information about the target including telephone-number, names, email addresses, etc.

Footprint: Having an idea about target’s IT architecture such as ip ranges, which ip address is active, which port is opening, OS, etc.

Vuln Analysis: Analysing and finding the vulnerabilities in target’s services or applications like network sniffing and spoofing, XSS, etc.

Exploitation: This is step you enter the target after analysing and find out weaknesses using tools such as Metasploit.

Post Exploitation: this step often is not allowed to be a part of pentest because of the risk of destabilising operational IT systems, therefore, post exploitation actions or clean up are also not performed.

What are the minimal requirements for a good pentest contract and pentest report?

For a good pentest contract, it should contain:

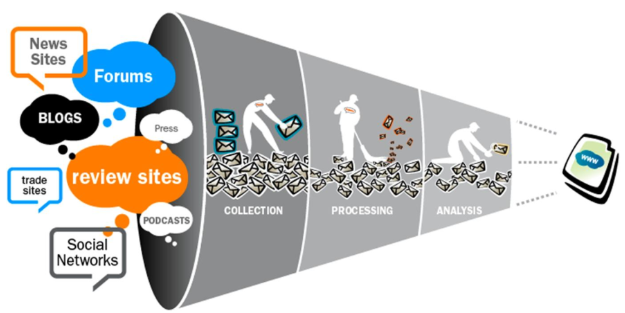
* A compensation clause which is signed by the client to show that you are allowed to check and resolve liability. It is normal and necessary to agree that, although the responsibility of careful testing rests with the inspector, all remaining risks in the inspection are for the customer. The tester is not responsible for any damage caused by the test!
* A confidentially agreement which must be signed by all testers participating in.
* Information about the scope, tested system as well as environment( location, ip-range, dns, website, etc).
* Test origin (ip-address from where tests will be performed, in our case the seclab's public ip) and test time so that customers can track it and be able to differentiate your tests from real attacks.
* Escalation procedures in case of incident / emergency

On the other hand, a good report should provide a goal of pentest, explaination of test approach and overall conclusion through documentations and a presentation.

The differences between a pent-test methodology and the cyber kill chain?

|  |  |
| --- | --- |
| Pen-test methodology | Cyber kill chain |
| a step-by-step approach to perform a pentest of a computer network / web-application / other IT equipment or software.  PTES defines penetration testing as 7 phases.   * Pre-engagement Interactions * Intelligence Gathering * Threat Modeling * Vulnerability Analysis * Exploitation * Post Exploitation * Reporting | Cyber kill chain is used for the identification and prevention of cyber intrusions activity.  Cyber kill chain defines 7 basic steps:   * External reconnaissance * Weaponization and packaging * Delivery * Exploitation * Installation * Command and Control * Actions on Targets |

# 4.Footprinting/Reconnaissance and Social Engineering



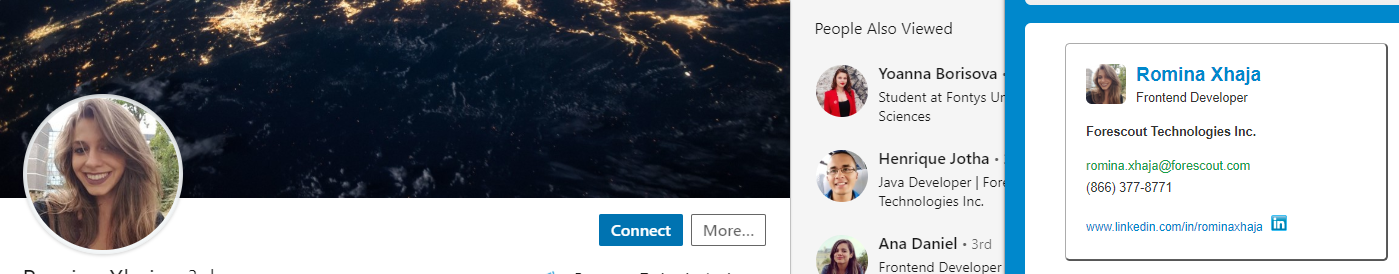
Footprinting(also known as reconnaissance) is the technique that is used to collect information about computer systems and what belongs to it. Various tools can be used to get that information that helps hackers a lot to crack systems. Generally, footprinting seems as a pre-attack phase because hacker uses footprinting to get the target’s information and provide them for the next step in the hacking process. This step seems to be an important step before doing pentest because the more information about target we gather, the more details we can do in pentest that means more vulnerabilities can be found.

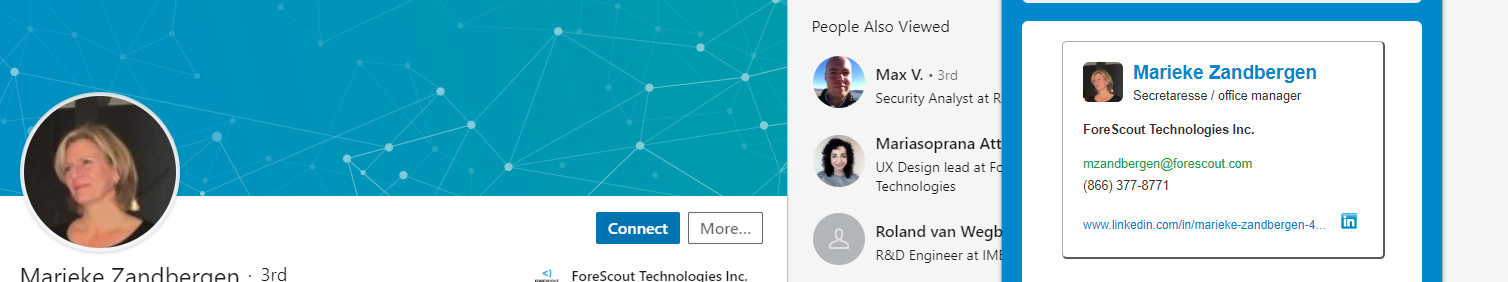
“Social Engineering/Hacking refers to psychological manipulation of people into performing actions or divulging confidential information” cited from Wikipedia. Social Engineering often is not allowed in pentest because of regarding as fraud.

Challenges:

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

I use an extension on google chrome to find out.







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

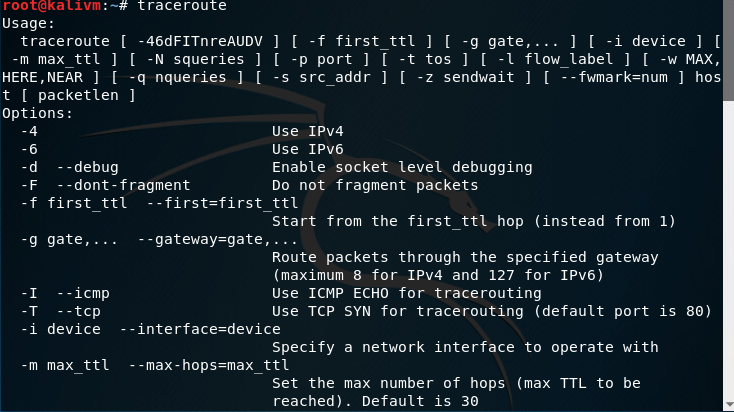


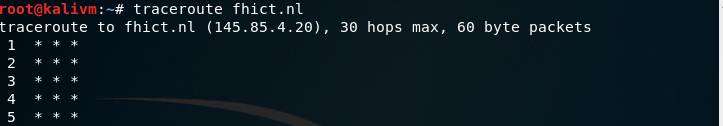
**Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.**

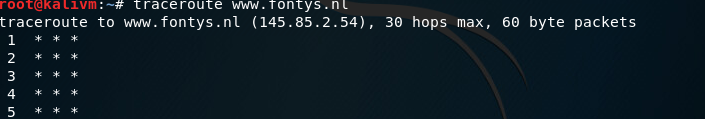
**Use kali for:**

* **traceroute to determine path to fontys.nl, fhict.nl**

Traceroute command is used to show several details about path that a packet takes from the computer we are on to the destination and it has many options.







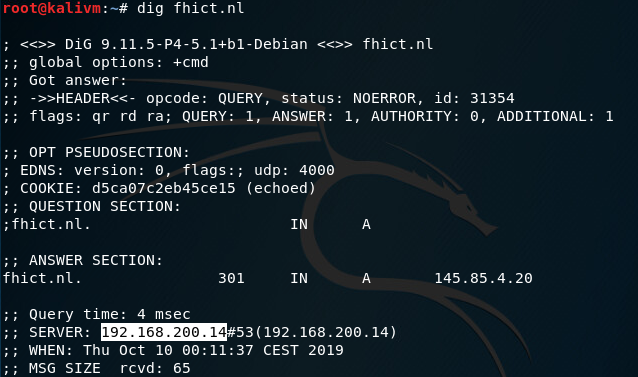
* **determine which DNS and email servers are used by fontys and fhict**

I used command dig to find out DNS servers.

**dig fontys.nl**

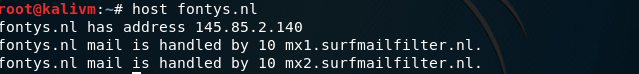


**Dig fhict.nl**



To find out email server, I used host command

**Host fontys.nl**



**Host fhict.nl**



* **determine which ip-adressess are used by fhict by whois utility and non whois tool**

Determine by whois tool

whois is a query what will response protocol that is widely used for querying databases that store the registered users such as a domain name, Ip.

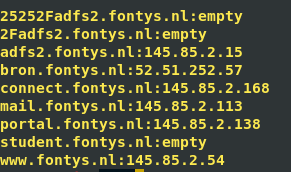
I tried whois fhict.nl command and cannot get anything. In my opinion, I thought that fhict.nl is more secured than before so whois command is no longer available to used.



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

With theharester, we can collect emails, subdomains, hosts, employee names, open ports and banner from different source.





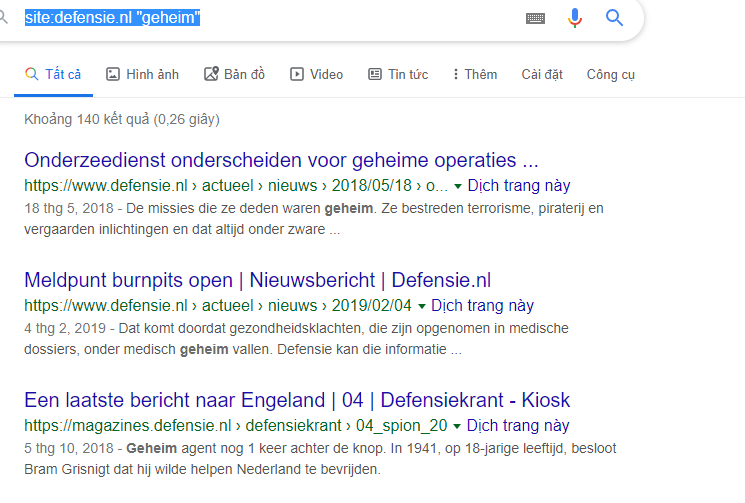
With this tool, I can find out many information about fontys.nl with only simple command

**Theharvester –d fontys.nl –b google**

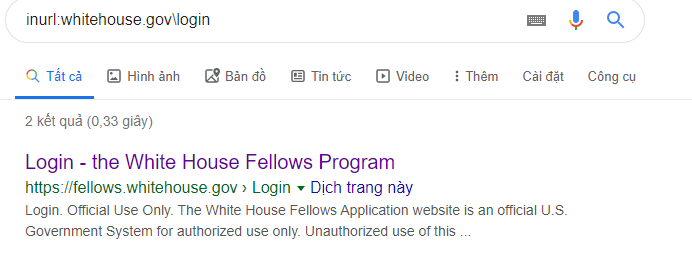
* **Discover contents of Google Hacking database**

First of all, what is Google hacking database? It is the biggest database of exploits and it is really powerful for script kiddies. It includes using operators in search engine of Google to determine specific string of text in the search results.

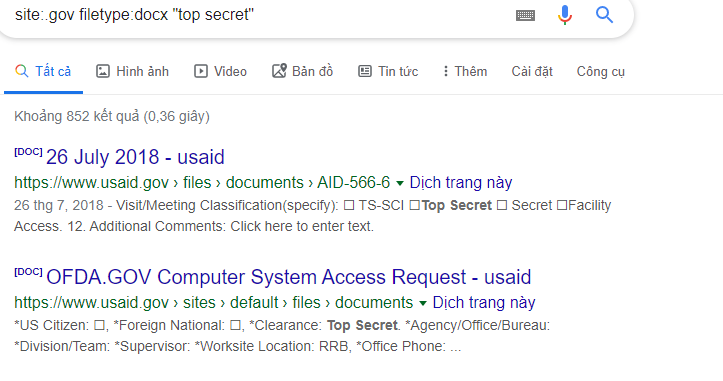
For example, as you can see below I use operator site to find out website defensive.nl and all the articles containing word “geheim”.



Furthermore, I also can find out log in page of whitehouse.gov website with inurl command:



Or for more specific, I am also able to use multiple operators for searching command



# 5.Network Scanning and Enumeration

Scanning a network or machine helps you to have a better view of a strange environment look like. The most popular tool is n-map, however, this tool will make lots of data on the network exposed including top-secret data.

**How a TCP(Transmission control protocol) communication session is set up?**

TCP uses a three-way hand shake (SYN,SYN-ACK,ACK) to establish a connection. The sever must figure out, bind and listen at a port to open connection. When this connection is established a client may start an active open. For more details, these are 3-way handshakes:

Syn: The active open will be executed when the client performs sending a SYN to the server. The client sets value A to the segment’s sequence number randomly.

Syn-ACK: In response, the server will reply with a Syn-Ack. The Acknowledgement number is set to one more than sequence number which just received(A+1) and the server will choose another random number for the packet B.

ACK: Lastly, ack will be sent back to the server. The sequence number is set to received acknowledgement value(A+1) and old acknowledgement number is set to one or more than the received sequence number(B+1).

**Difference type of portscanning**

With n-map, many type of scanning can be used and each of them has a specific purpose. For example, TCP SYN scan or TCP connect Scan is used to scanning thousand of ports per second on a fast network not hampered by restrictive firewalls. On the other hand, to determine which IP protocols are supported on the target’s network the command –So will be used. As I mention above, n-map is really useful but also dangerous, therefore, this tool must be put into consideration before use.

**Different results you can get for a tcp (or udp)**

Nmap can recognize 6 port states so there are results we could get for a TCP or even UDP. For example, when Nmap command is executed, all TCP ports, TCP status, and service are shown on the screen and it also occurs with UDP.

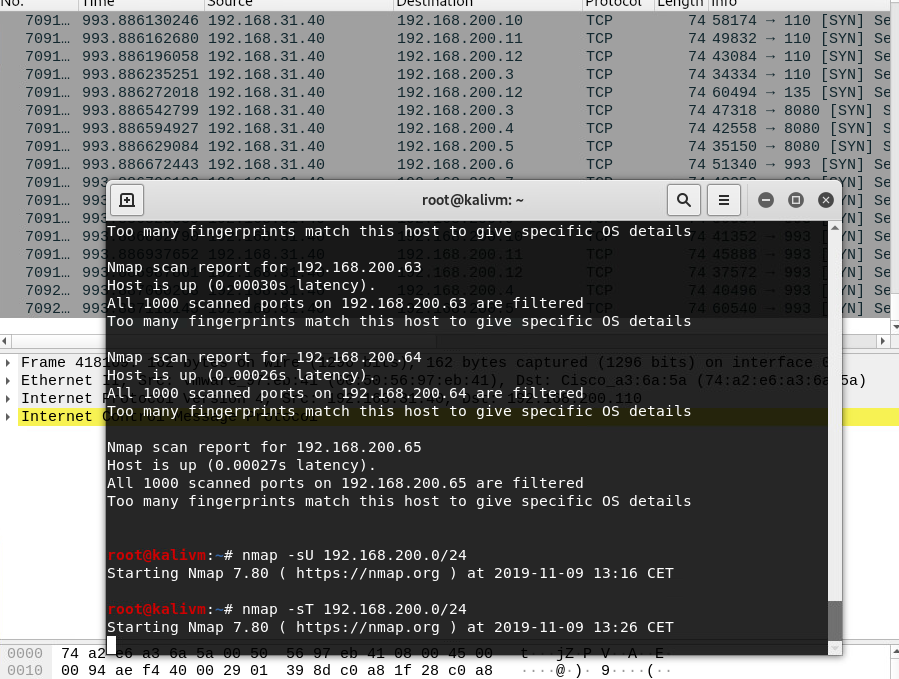
**Detect OS**

One of the Nmap’s best-known features is found out OS detection. When nmap is executed, a series of TCP and UDP packets will be sent to the remote host and check every bit in responses. After that, IP ID sampling, Nmap will compare the results to its nmap-os-db database of more than 2600 known OS and give the result to the screen if it matches. OS detection is very useful for exploiting source-IP based trust relationship or for hiding the source of an attack. Although this kind of spoofing is rarely performed now, it still has certain amount of dangerous points.

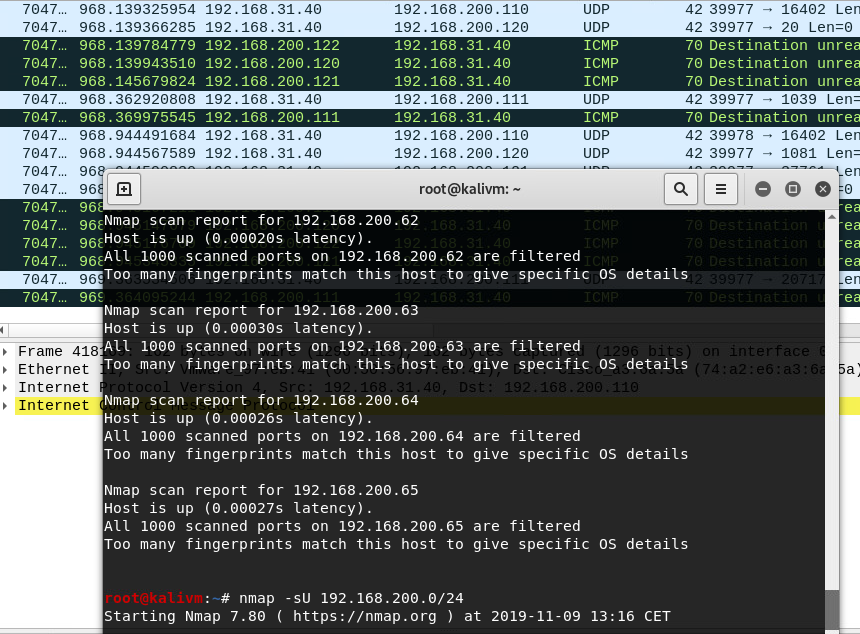
**Challenges**

I did 3 type of nmap Scan for network 200:192.168.200.0/24

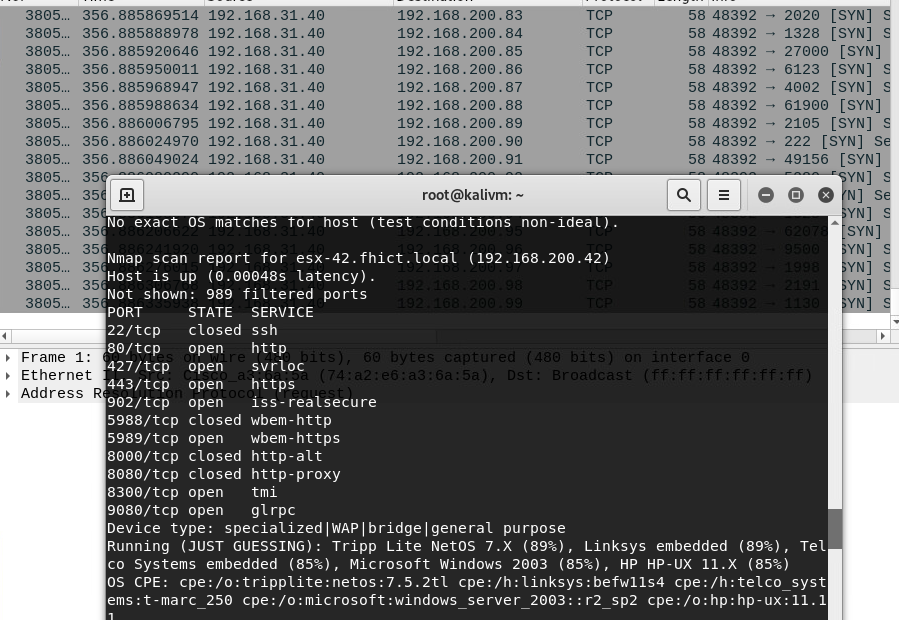
-TCP Scan



-UDP Scan

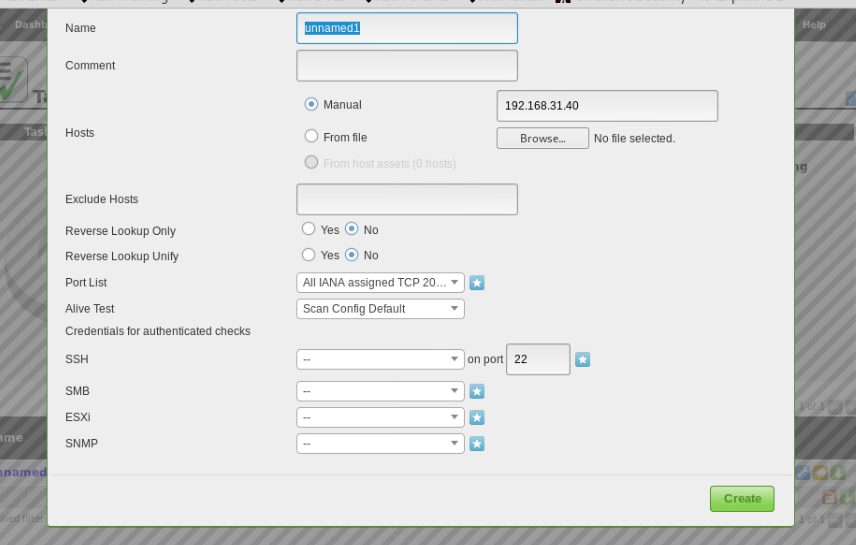


-OS Scan



Through all results I got after scanning I can see what ip is up, what port is opening.

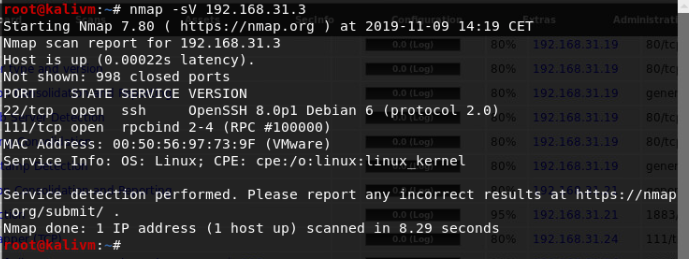
I also tried using OpenVAS to scan network 32 which is being used on my test environment.



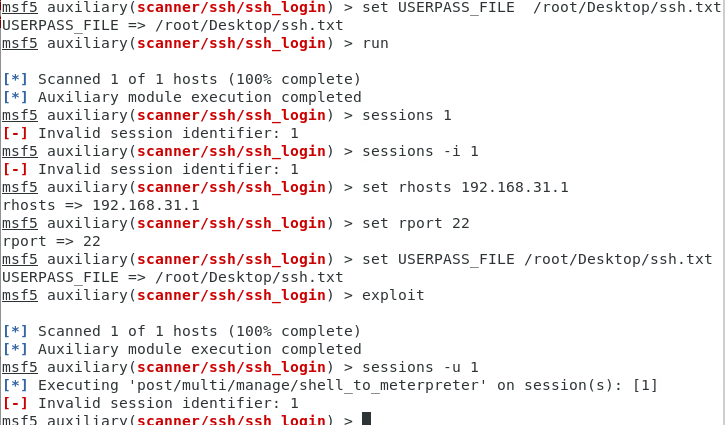
After about 15 minutes of Scanning, many vulnerabilities are exposed.



I saw that ip 192.168.31.3 has vulnerability about ssh and I tried scanning it with nmap.

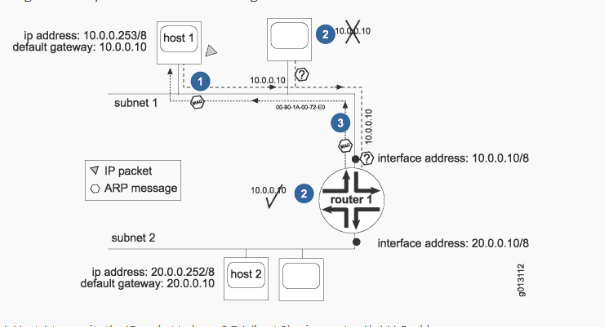


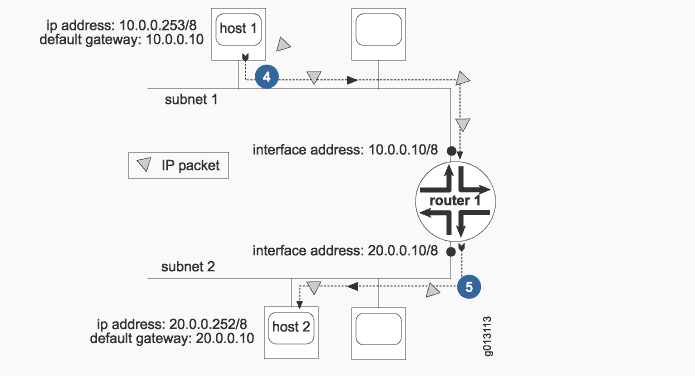
Next,I tried finding valid credential but unfortunately I cannot find out.



# 6.Network Sniffing and Spoofing

Before going to the core knowledge about this, I would like to show how ARP(Address Resolution Protocol) work first.





A typical scenario is:

Host 1 runs an ARP request to all devices on subnet 1 , created by a query with the IP of router 1. Because host 2 is on another network so the IP address of router 1 is necessary. All the devices on subnet 1 will compare their own IP with the enclosed IP sent by host 1. If match, router 1 will send an ARP response including its MAC to host 1. Host 1 transmits the IP packet to layer 3 in host 2 using MAC address of router 1 then Router 1 will forward IP packer to host 2. Router 1 might send an ARP request to identify the MAC of host 2. All receiving hosts is forced to compare their IP with the IP of the the ARP request. If host 1 sends another IP packet to host 2, host 1 will searches its ARP table for the router 1 MAC address.

Then If the default router or gateway becomes unavailable, then all the packets forwarding to remote destinations will be stopped.

**Sniffing**

Sniffing sounds like an illegal action when it seems to be an eavesdropping act between digital communication parties such as wired laptop and wired switch on local area. For all retrieved information, hacker can use them to retrieve more information and do evil things.

There are two types of Sniffing are:

Active Sniffing: Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic.

Passive Sniffing: This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

The most common tool used to sniff is Wireshark.

**Spoofing**

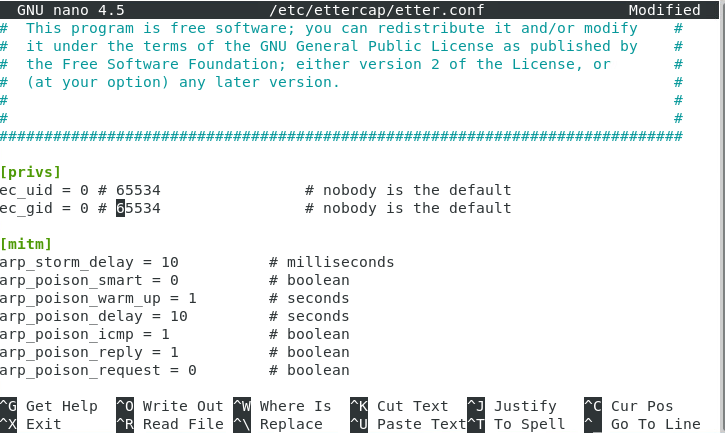
Spoofing is the act of pretending to be another person/system to do illegal thing such as sending an e-mail, TCP/IP, ARP or DNS with an address which is not yours.

**ARP Spoofing**

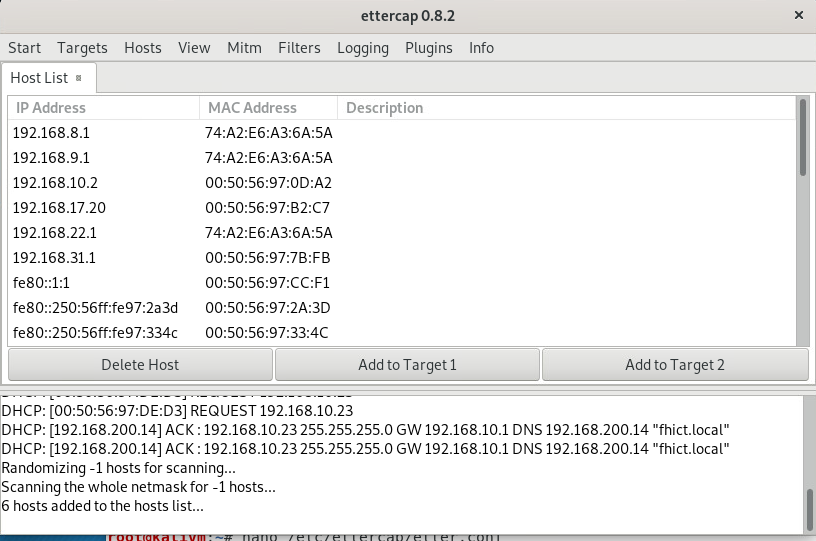
ARP Spoofing allows an intruder/hacker to block data on the network, modify the traffic or stop all traffic. ARP Spoofing seems to be a prelude to other attacks such as DDOS, Men-in-the-middle or interchain robbery attacks. This attack can only be used on networks that use ARP. Because ARP does not provide methods for authenticating ARP replies on the network, ARP responses may come from systems other than the one that has a second-floor address required. Additionally, a host can accept ARP reply packet without sending the ARP request pack. Taking advantage of this issue, hacker can deploy attack methods as I mentioned above.

**Challenge**

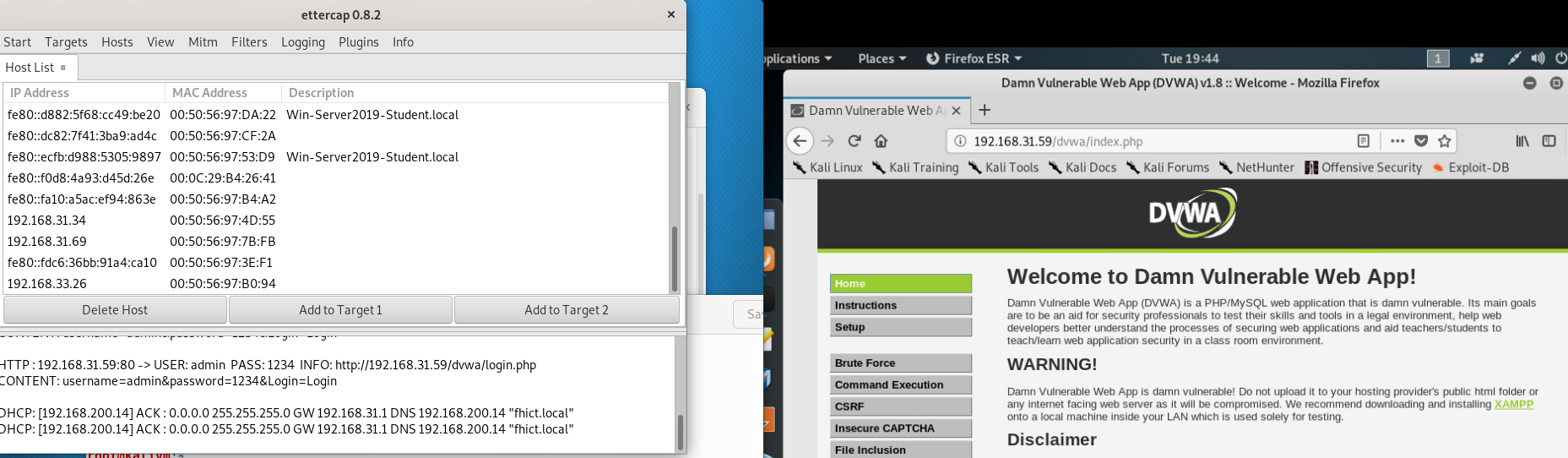
I set up file Ettercap.conf to listen to VLAN 31 as below:



Then I used Ettercap to scan and deploy ARP poison to attack.



Luckily, while I was scanning, 1 host was caught when trying to log in an unsecured website.



I also tried doing Man-In-The-Middle to other secured website but I failed. With https, these websites are safe from sslstrip, therefore, I cannot attack.

# 7.SQL INJECTION

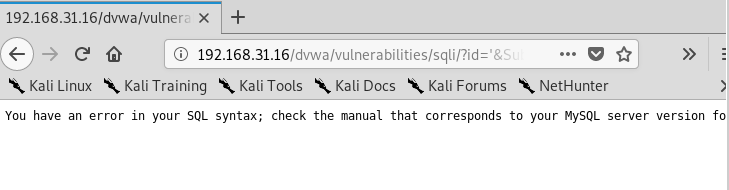
SQL injection is a technique that allows attackers to take advantage of the vulnerability of checking input data in web applications and error messages returned by the database management system to inject. and executing illegal SQL statements. SQL injection can allow attackers to perform operations, delete, insert, update, etc. on the database of the application, even the server it is running on. SQL injection is commonly known as an attacker on web applications whose data is managed by database management systems such as SQL Server, MySQL, Oracle, DB2, Sysbase, etc.

I did some test on DVWA.

Firstly, I took easy level.

1.Check for vulnerability

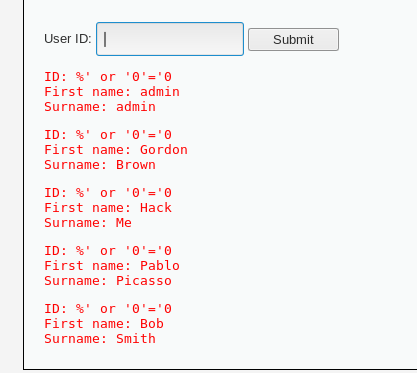
When I added quote to the url, I got error like the image below that means website is vulnerable to sql injection



2.Always true test

I fill in textbox with ‘%’ or ‘0’=’0’ that equals to

SELECT first\_name, last\_name FROM users WHERE user\_id = '**%' or '0'='0'**;

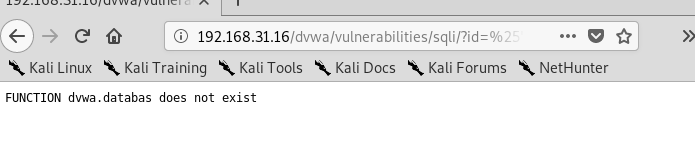


3.Display database name

Next, I decided to find out database name to help me dig deep into information.

%' or 0=0 union select null, database() #

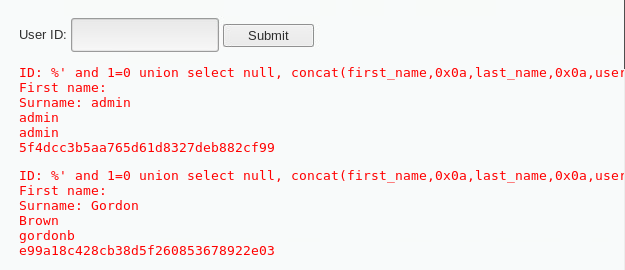
I use this command in textbox.



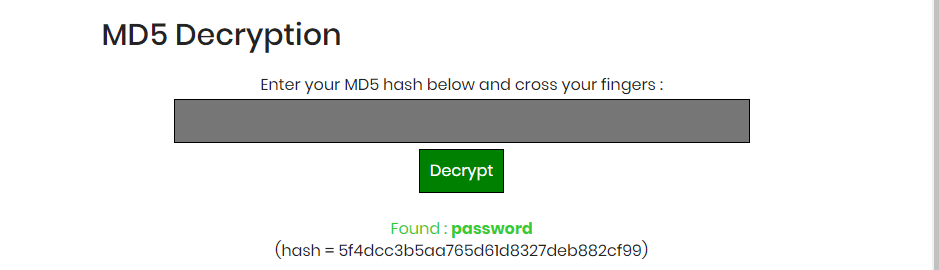
4.Display all the columns fields and information of user table

This command will help me get necessary authentication information from database:

%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #



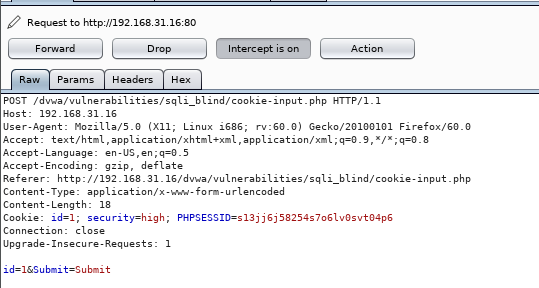
Then I use md5 decrypt to convert md5 code to text.Tada!!! I got password for admin.



Next level, I decided to get more challenge by doing Blind SQLi in high level in DVWA environment.

1. Run Burpsuit

I use burpsuit to see what was happening while I click submit button



Then I got phpsessid as an important information(The browser stores this PHPSESSID, so that each time the browser accesses it, it sends PHPSESSID back to PHP.

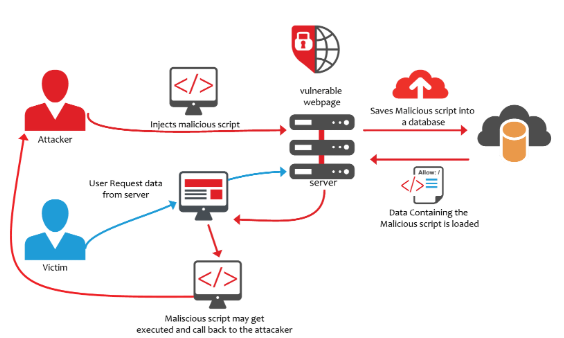
PHP relies on the incoming PHPSESSID to recover - retrieving data from the file is SESSION's information).

1. Using sqlmap



I tried to get information through sqlmap but it did not work.

# 8. XSS( Cross-Site Scripting)

Cross Site Scripting (XSS) is one of the most common and vulnerable attacks that all experienced Testers know about. It is considered one of the most dangerous attacks on web applications and can have serious consequences. Introduction to XSS attack XSS attack is a malicious code, to exploit an XSS vulnerability, hackers will insert malicious code through scripts to execute them on the client. Typically, XSS attacks are used to bypass user access and impersonation.

The main purpose of this attack is to steal user identification data such as cookies, session tokens and other information. In most cases, this attack is being used to steal other people's cookies. As we know, cookies help us log in automatically. Therefore with stolen cookies, we may log in with other identifying information. And this is one of the reasons, why this attack is considered one of the most dangerous attacks.

XSS attack is being performed on the client side. It can be done with different client-side programming languages. However, most often this attack is carried out with Javascript and HTML.

How does it work?

Cross Site Scripting attack means sending and inserting malicious commands and scripts, these malicious codes are often written with client-side programming languages ​​such as Javascript, HTML, VBScript, Flash ... However, this attack is usually used Javascript and HTML. This attack can be performed in different ways, depending on the type of XSS attack, which can be reflected in the victim's browser or stored in the database and run each time. when the user calls the appropriate function. The main cause of this type of attack is user input data validation mismatch, malicious data from input can penetrate the output data. Malicious code could enter a script and be inserted into the source code of a website. Then the browser cannot know if the executable code is malicious or not. Thus malicious code may be being executed on the victim's browser or any other form of counterfeit is being displayed to the user. There are several types of XSS attacks that can occur. There are three types of XSS attack:

-Reflected XSS

-Stored XSS

-Dom Bases XSS

*Reflected XSS and Stored XSS have two major differences during the attack.*

First, to exploit Reflected XSS, a hacker must trick the victim into accessing his or her URL. Stored XSS does not need to do this, after inserting dangerous code into the application's database, hackers just wait for the victim to automatically access. For the victim, this is completely normal because they are unaware that the data they have accessed has been contaminated.

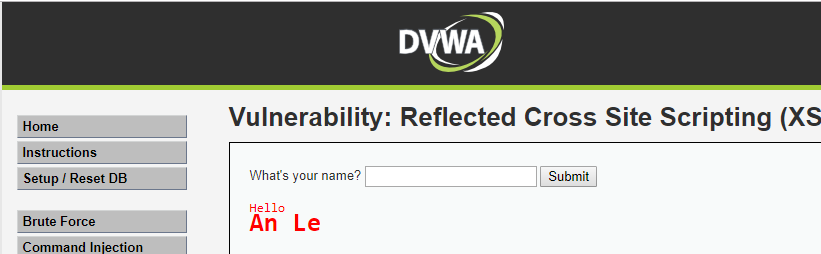
Second, the target of the hacker will be easier to achieve if at the time of attack the victim is still in the session of the web application. With Reflected XSS, a hacker can persuade or trick a victim into logging in and then accessing the URL he provides to execute malicious code. But Stored XSS is different, because the malicious code is stored in the Web database so whenever the user accesses related functions, the malicious code will be executed, and most likely these functions require authentication. Real (logon) first should be obvious during this time the user is still in the session.

From these things, it can be seen that Stored XSS is much more dangerous than Reflected XSS, the affected object can be all but the users of that web application

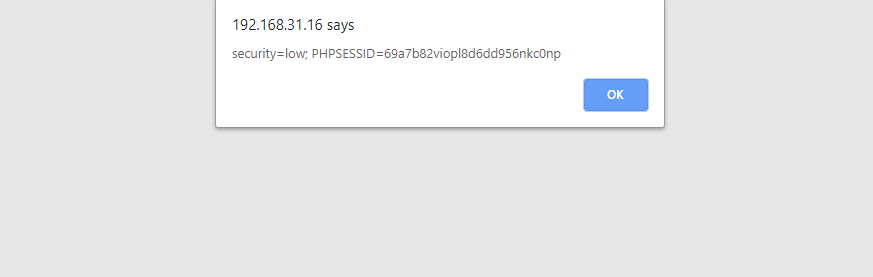
**a. Reflected XSS**

There are many ways to exploit it through the Reflected XSS error, one of the best known is to take a user's session, thereby being able to access data and gain their rights on the website.

firstly, I used h1 html tag to test if this website is vulnerable.



After knowing this website is vulnerable to XSS, I use command to get cookie.



For higher lever, I used body tag(upper case, lower case) to do such as:

**<body onload=alert(document.cookie)>**

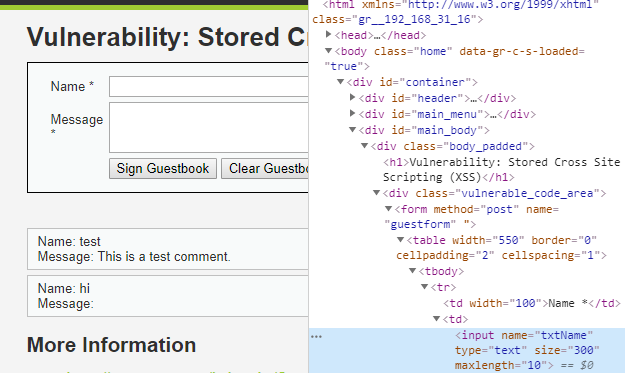
**b. Stored Xss**

Unlike Reflected, which attacks directly on a number of victims targeted by hackers, Stored XSS targets more victims. This error occurs when the web application does not double-check the input data before saving to the database (here I use this concept to refer to the database, file or other areas to store application data). web application). For example, the comments form comments ... on the website. With Stored XSS technology, hackers do not exploit directly but must perform at least 2 steps.

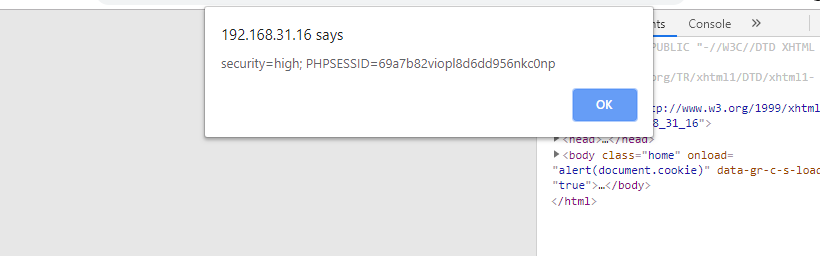
First, the hacker will approve the input points (form, input, textarea ...) that have not been carefully checked to insert into the database dangerous codes.

Next, when the user accesses the web application and performs operations related to this saved data, the hacker code will be executed on the user's browser.

Firstly, I change some HTML codes(size of textbox, maxlength) because for high level textbox limits the input characters:



After that, it becomes easier to get cookie from website.



# 9. CSRF( Cross-Site Request Forgery)

CSRF (Cross Site Request Forgery) is a technique that attacks by using a user's authentication authority on a website. CSRF is a technique to attack users, based on which hackers can perform operations that require authentication. In a nutshell, this is an attack technique based on unauthorized borrowing.

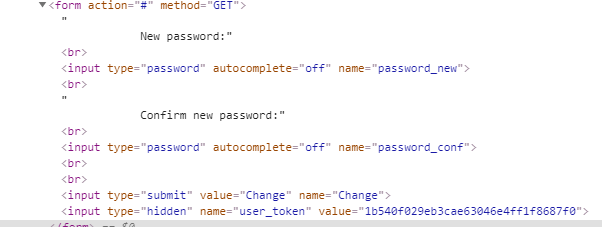
Web applications operate by receiving HTTP commands from the user, then executing them. Hackers use the CSRF method to trick the user's browser to send http commands to web applications. This can be done by inserting malicious code or linking to websites that the user has already authenticated. In the event that the user's session has not expired, the above commands will be executed with the user's authentication rights.

Example:

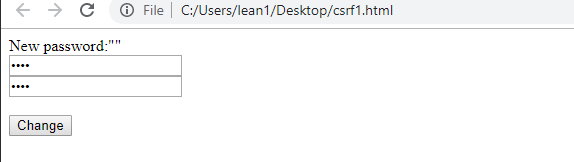
I change password for user Admin in dvwa website to 1234 and I get usertoken.

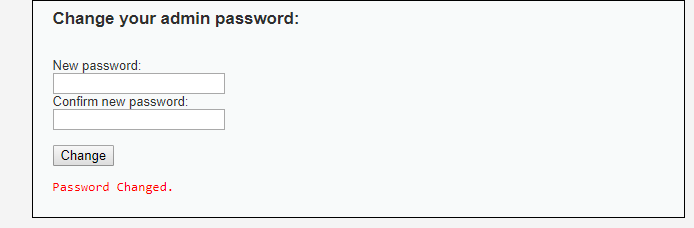


Then I make another html file with method GET that similar to this function.

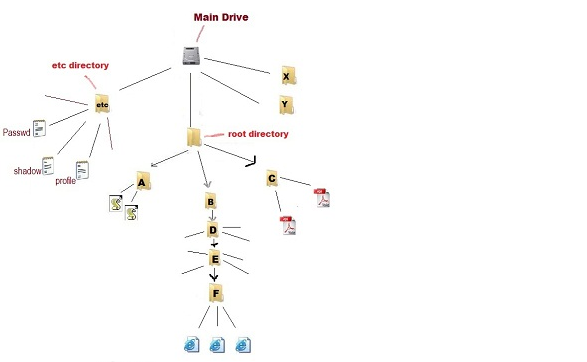


Next,save this file as html file and run it then it works.





# 10. Path traversal, (remote) file inclusion and command injection



Path traversal (also known as Directory traversal) is a type of attack that allows hackers to access directories and resource files outside the current directory. These unauthorized resources may include source code, server configuration information, system files, and directories, etc.

In addition, this vulnerability is often combined with a number of other vulnerabilities to enable further exploitation.

This is a very dangerous flaw because it can affect the system. At a simple level, hackers can read files in web directories or even sensitive files in the system.

Example:

Assuming the image files are saved **in / var / www / html / blog / public / img /**

When accessing the file avatar.jpg on this folder dev can link to GET photo / file? Name = avatar.jpg. Now the webserver will access the file at **/var/www/html/blog/public/img/avatar.jpg** and return it to the user.

But instead of passing the file name as avatar.jpg, the hacker could pass the file name as **../../../../../../etc/password**. Now the webserver will access and return the file at **/var/www/html/blog/public/img/../../../../../../etc/password**. This path is equivalent to **/ etc / pasword** so the webserver will return the file system.

# 11. Password cracking

In password analysis and computer security, password cracking is the process of recovering passwords from data stored in or transmitted by a computer system. A common approach (brute-force attack) is to continually try to guess passwords and check them against the password's built-in hash function. [first]

The purpose of password cracking can be to help users recover a forgotten password (setting a completely new password is less likely to pose a security risk, but it involves a System Administrator privilege), so that unauthorized access to the system or act as a precautionary measure whereby system administrators check for passwords that are vulnerable to cracking. On a file-by-file basis, password cracking is used to gain access to digital evidence that a judge has authorized access to, when the rights of a specific file are limited.

There are some types of cracking password:k

-Dictionary Attacks: An attack dictionary is a complete text file of commonly used passwords or a list of all the words in the dictionary used to fight the password database. Strong passwords are often not vulnerable to this type of attack.

-Brute-force Attacks: In theory, this method can crack every password. It will try every possible combination of characters, numbers, special characters until the correct password is found. This method takes a lot of time. The attack speed is determined by the speed of the computer running the crack program and the difficulty of the password.

- Hybrid Attacks: As the next level of hackers, an attempt if passwords cannot be found using Dictionary Attack. Hybrid attacks start with a dictionary file and replace the numbers and symbols for characters in the password. For example, many users add number 1 to their password to meet the strong password requirements. Hybrid is designed to look for unusual types in passwords

References:

<https://en.wikipedia.org/wiki/Responsible_disclosure>

<https://www.hackerone.com/disclosure-guidelines>

[https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Law-24-2018-QH14-Cybersecurity-388829.aspx (vietnamese](https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Law-24-2018-QH14-Cybersecurity-388829.aspx%20(vietnamese) website)

<http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf>

<https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html>

<https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-EN.pdf>

[https://nmap.org](https://nmap.org/)

<https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types>

<https://en.wikipedia.org/wiki/ARP_spoofing>

<https://www.owasp.org/index.php/Path_Traversal>