**Basic Knowledge Assignment**

**Made by:** Tim Chermin

**Version:** 1.0

**Date:** 13/09/2019

Table of Contents

[Introduction 3](#_Toc19281835)

[Version 5](#_Toc19281836)

[Subjects 5](#_Toc19281837)

[Law, Ethics and Responsible Disclosure 5](#_Toc19281838)

[Basic Hacking Process 5](#_Toc19281839)

[Relevance 5](#_Toc19281840)

[Starting point 5](#_Toc19281841)

[Approach 6](#_Toc19281842)

[Background information 6](#_Toc19281843)

[Execution 8](#_Toc19281844)

[Afterthoughts 8](#_Toc19281845)

[Sources 8](#_Toc19281846)

[Social Engineering and Foot printing 8](#_Toc19281847)

[Network Scanning and Enumeration 9](#_Toc19281848)

[Network Sniffing and Spoofing 9](#_Toc19281849)

[SQL Injection 9](#_Toc19281850)

[XSS 10](#_Toc19281851)

[CSRF 10](#_Toc19281852)

[Path Traversal, File inclusion and Command Injection 10](#_Toc19281853)

[Password Cracking (system and network) 11](#_Toc19281854)

[Wireless Hacking 11](#_Toc19281855)

[Tooling (VMWare ESX and Seclab, Wireshark, Linux basic skills, Web application Proxy & browser tools) 11](#_Toc19281856)

[Final Conclusion and Reflection from the first ten weeks 16](#_Toc19281857)

# Version

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Autor** | **Date** | **Changes** |
| 1.0 | Tim Chermin | 13/09/2019 | * Basic setup * Start of Basic Hacking Process added * Start of linux added |
|  |  |  |  |
|  |  |  |  |

# 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 hopping to learn as much of the basics as I possibly can.

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

# Subjects

## Law, Ethics and Responsible Disclosure

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

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

## Basic Hacking Process

### Relevance

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

### Starting point

My prior knowledge concerning the basic hacking process:

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

### Approach

I’ll start with following the instruction about this subject and after the instruction I’ll gather 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, dialers 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 al the findings in the test. In the presentation the tester will explain all his findings and conclusions in front of the client. While the report will contain the coals and the scope of the test, an explanation of the test approach, the results of the test and overall conclusions. These conclusions also include advise on how to solve some of the issues.

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

**Similarities:**

* Intelligence gathering
* Exploitation

**Differences:**

* Installing malware
* Fishing mail

### Execution

#### Practice environment

### Afterthoughts

 **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)

### 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

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

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

## Network Scanning and Enumeration

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

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

## Network Sniffing and Spoofing

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

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

## SQL Injection

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

‘OR ‘1’ = ‘1

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

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

## XSS

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

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

## CSRF

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

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

## Path Traversal, File inclusion and Command Injection

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

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

## Password Cracking (system and network)

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

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

## Wireless Hacking

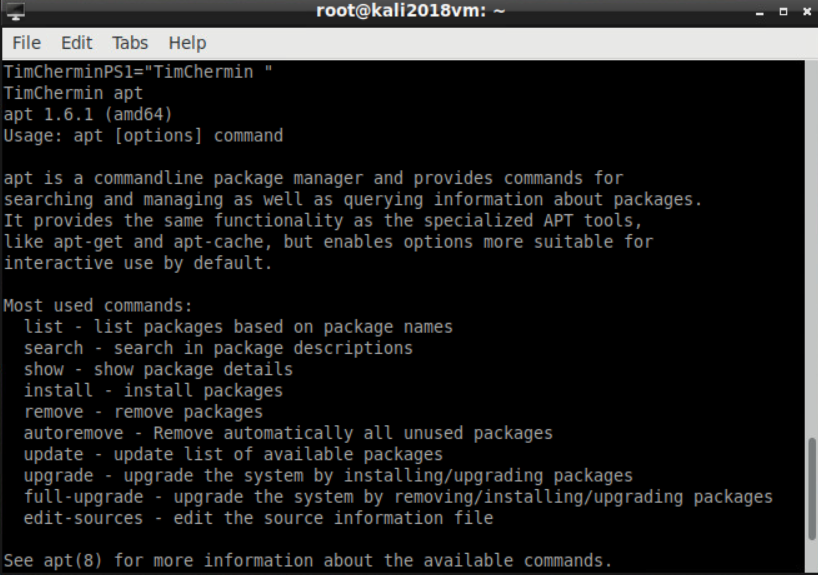
 **Per Subject (from above mentioned subjects in "*1) Introduction Assignment*"):**

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

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

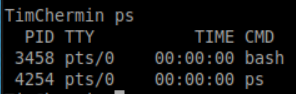
**Linux basic skills:**

**Command line activities:**

**APT:** 

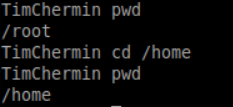
The CLI's apt command lets you search for, install, and remove software and add new repositories with relative ease. When you use the **apt** command, you can be sure that you're seeing all the applications available in the repositories, whereas the software manager doesn't necessarily catch them all.

**PS command:**



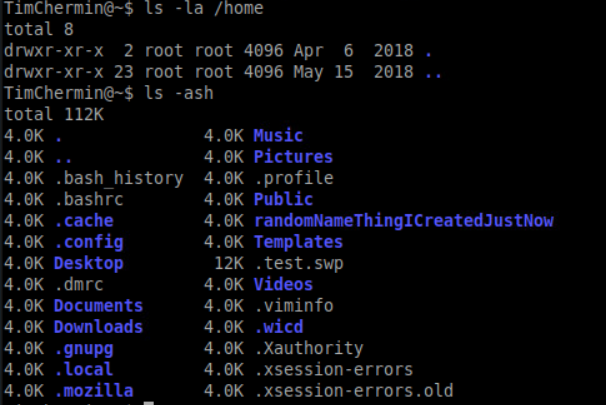
the [**ps** command](https://www.lifewire.com/uses-of-linux-ps-command-4058715) can show all processes; show all processes except session leaders; and show all processes except session leaders and those not associated with a terminal. The **ps** command can also show all processes associated with this terminal or, indeed, any other; restrict the output to only running processes; and show only the processes for a specific command, or for a specific group of users or user. In all, there are hundreds of different ways to format, view, and present the list of processes running on your system using the **ps** command — and that is just one command.

**Pwd:**

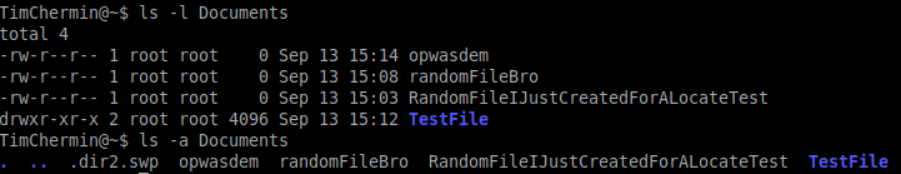


Use the **pwd** command to print the working directory (the current directory you are in).

**ls -la /home**

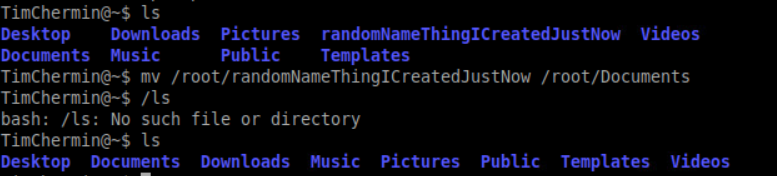


Lists ALL the files and directories in the /home directory, in the long listing format.

**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.

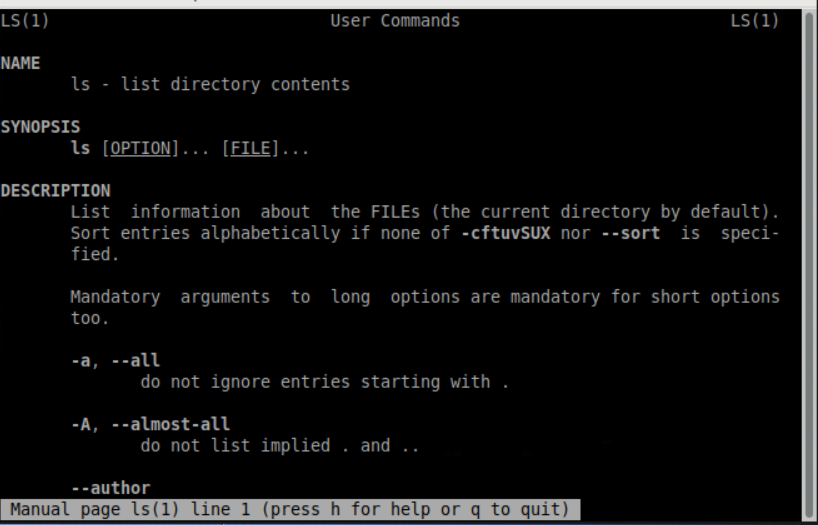
**Mv:**



The mv command - move - allows a user to move a file to another folder or directory. Just like dragging a file located on a PC desktop to a folder stored within the "Documents" folder, the mv command functions in the same manner. An example of the mv command is:

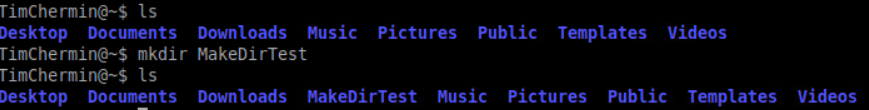
**Man:**

**Man ls**

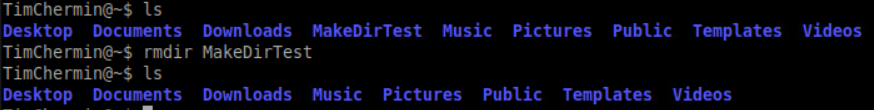


The man command - the manual command - is used to show the manual of the inputted command. Just like a film on the nature of film, the man command is the meta command of the [Linux CLI](http://www.informit.com/articles/article.aspx?p=1339466). Inputting the man command will show you all information about the command you are using. An example:

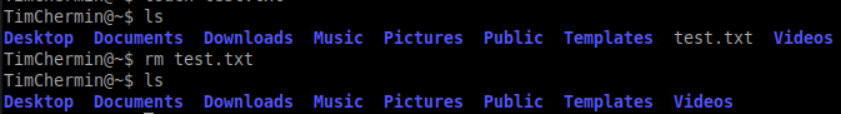
**Mkdir & rmdir & rm:**



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. An example of the mkdir command



The rmdir - remove directory - command allows the user to remove an existing command using the Linux CLI. An example of the rmdir command:



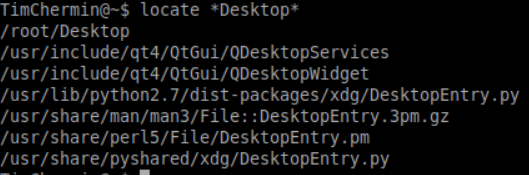
The rm command - remove - like the rmdir command is meant to remove files from your Linux OS. Whereas the rmdir command will remove directories and files held within, the rm command will delete created files. An example of the rm command:

**Touch:**



The touch command - a.k.a. the make file command - allows users to make files using the Linux CLI. Just as the mkdir command makes directories, the touch command makes files. Just as you would make a .doc or a .txt using a PC desktop, the touch command makes empty files. An example of the touch command:

**Locate:**



The locate - a.k.a. find - command is meant to find a file within the Linux OS. If you don't know the name of a certain file or you aren't sure where the file is saved and stored, the locate command comes in handy. A locate command example:

Learning and accountability:

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

PS1="YourInitials@\w\$ "

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

**Sources:**

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

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

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

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

 **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)