**Basic Knowledge Assignment**

**Made by:** Tim Chermin

**Version:** 1.0

**Date:** 06/09/2019

Table of Contents

[Introduction 3](#_Toc18668707)

[Subjects 4](#_Toc18668708)

[Law, Ethics and Responsible Disclosure 4](#_Toc18668709)

[Basic Hacking Process 4](#_Toc18668710)

[Relevance 4](#_Toc18668711)

[Starting point 4](#_Toc18668712)

[Approach 4](#_Toc18668713)

[Background information 4](#_Toc18668714)

[Execution 5](#_Toc18668715)

[Afterthoughts 5](#_Toc18668716)

[Social Engineering and Foot printing 5](#_Toc18668717)

[Network Scanning and Enumeration 5](#_Toc18668718)

[Network Sniffing and Spoofing 6](#_Toc18668719)

[SQL Injection 6](#_Toc18668720)

[XSS 6](#_Toc18668721)

[CSRF 7](#_Toc18668722)

[Path Traversal, File inclusion and Command Injection 7](#_Toc18668723)

[Password Cracking (system and network) 7](#_Toc18668724)

[Wireless Hacking 8](#_Toc18668725)

[Tooling (VMWare ESX and Seclab, Wireshark, Linux basic skills, Web application Proxy & browser tools) 8](#_Toc18668726)

[Final Conclusion and Reflection from the first ten weeks 8](#_Toc18668727)

# Introduction

* What was your relevant prior knowledge and experience on security, Linux and networking or what did you do to obtain this knowledge?
* What was your preferred learning style?
* What were your personal learning goals?

# 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 thought 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*"):**

* 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)

 **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)