# Pentesting Methodology

## 0- Physical Attacks

Do you have **physical access** to the machine that you want to attack? You should read some **tricks about physical attacks** and others about **escaping from GUI applications**.

## 1. Discovering hosts inside the network / Discovering Assets of the company

**Depending** if the **test** you are perform is an **internal or external test** you may be interested on finding **hosts inside the company network** (internal test) or **finding assets of the company on the internet** (external test).

Note that if you are performing an external test, once you manage to obtain access to the internal network of the company you should re-start this guide.

## 2. Having Fun with the network (Internal)

**This section only applies if you are performing an internal test.** Before attacking a host maybe you prefer to **steal some credentials from the network** or **sniff** some **data** to learn **passively/actively(MitM)** what can you find inside the network. You can read **Pentesting Network**.

## 3. Port Scan - Service discovery

The first thing to do when **looking for vulnerabilities in a host** is to know which **services are running** in which ports. Let's see the **basic tools to scan ports of hosts**.

## 4. Searching service version exploits

Once you know which services are running, and maybe their version, you have to **search for known vulnerabilities**. Maybe you get lucky and there is a exploit to give you a shell...

# 5. Pentesting Services

If there isn't any fancy exploit for any running service, you should look for **common misconfigurations in each service running.**

**Inside this book you will find a guide to pentest the most common services** (and others that aren't so common)**. Please, search in the left index the *PENTESTING* section** (the services are ordered by their default ports).

**I want to make a special mention of the Pentesting Web part (as it is the most extensive one).** Also, a small guide on how to **find known vulnerabilities in software** can be found here.

**If your service is not inside the index, search in Google** for other tutorials and **let me know if you want me to add it.** If you **can't find anything** in Google, perform your **own blind pentesting**, you could start by **connecting to the service, fuzzing it and reading the responses** (if any).

## *5.1 Automatic Tools*

There are also several tools that can perform **automatic vulnerabilities assessments**. **I would recommend you to try Legion, which is the tool that I have created and it's based on the notes about pentesting services that you can find in this book.**

## *5.2 Brute-Forcing services*

In some scenarios a **Brute-Force** could be useful to **compromise** a **service**. **Find here a CheatSheet of different services brute forcing**.

# 6. Phishing

If at this point you haven't found any interesting vulnerability you **may need to try some phishing** in order to get inside the network. You can read my phishing methodology:

# 7. Getting Shell

Somehow you should have found **some way to execute code** in the victim. Then, a list of possible tools inside the system that you can use to get a reverse shell would be very useful.

Specially in Windows you could need some help to **avoid antiviruses**:

# 8. Inside

If you have troubles with the shell, you can find here a small **compilation of the most useful commands** for pentesters:

- **Linux**
- **Windows (CMD)**
- **Winodows (PS)**

# 9. Exfiltration

You will probably need to **extract some data from the victim** or even **introduce something** (like privilege escalation scripts).

# 10. Privilege Escalation

## *10.1. Local Privesc*

If you are **not root/Administrator** inside the box, you should find a way to **escalate privileges.** Here you can find a **guide to escalate privileges locally in Linux and in Windows.** You should also check this pages about how does **Windows work**:

- **Authentication, Credentials, Token privileges and UAC**
- How does **NTLM works**
- How to **steal credentials** in Windows
- Some tricks about ***Active Directory***

**Don't forget to checkout the best tools to enumerate Windows and Linux local Privilege Escalation paths:** Suite PEAS

## *10.2. Domain Privesc*

Here you can find a **methodology explaining the most common actions to enumerate, escalate privileges and persist on an Active Directory**. Even if this is just a subsection of a section, this process could be **extremely delicate** on a Pentesting/Red Team assignment.

# 11. POST

## *11.1. Looting*

Check if you can find more **passwords** inside the host or if you have **access to other machines** with the **privileges** of your **user**. Find here different ways to **dump passwords in Windows**.

## *11.2. Persistence*

**Use 2 o 3 different types of persistence mechanism so you won't need to exploit the system again. Here you can find some persistence tricks on active directory.**

TODO: Complete persistence Post in Windows & Linux

# 12. Pivoting

With the **gathered credentials** you could have access to other machines, or maybe you need to **discover and scan new hosts** (start the Pentesting Methodology again) inside new networks where your victim is connected. In this case tunnelling could be necessary. Here you can find **a post talking about tunnelling**. You definitely should also check the post about Active Directory pentesting Methodology. There you will find cool tricks to move laterally, escalate privileges and dump credentials. Check also the page about **NTLM**, it could be very useful to pivot on Windows environments..

MORE

# *Android Applications*

# *Exploiting*

- **Basic Linux Exploiting**
- **Basic Windows Exploiting**
- **Basic exploiting tools**

*Basic Python*

*Crypto tricks*

- **ECB**
- **CBC-MAC**
- **Padding Oracle**