“Hacking with Metasploit” Tutorial

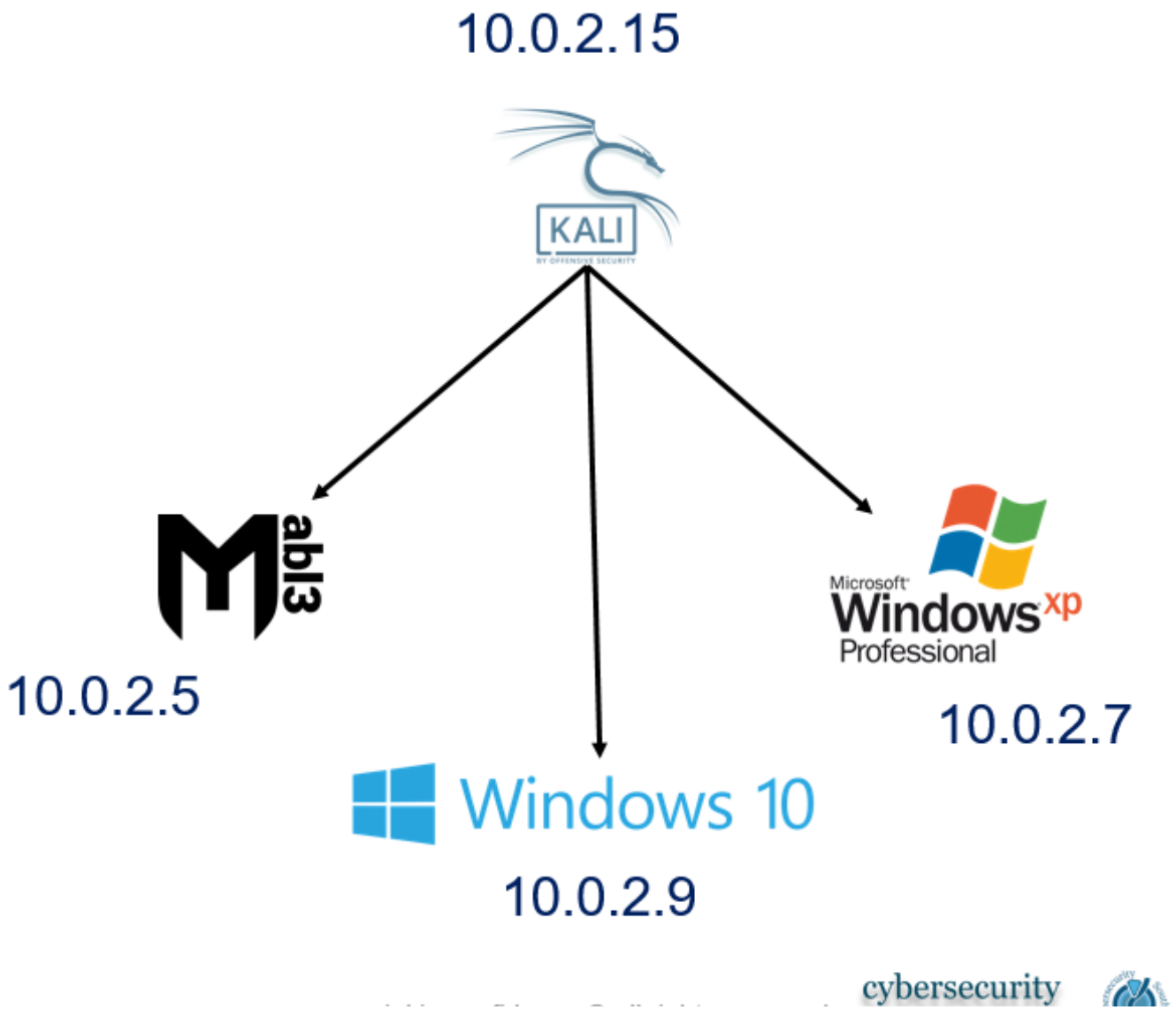
Federico Lombardi Follow
Apr 4 · 6 min read

Last 12th February (2019) I was invited to ITASEC, the annual Conference of Cybersecurity held in Italy. The event has been held at the CNR of Pisa with an incredible heterogeneous audience composed by a number of public administrations, researchers and industry from all over Europe.

The event lasted 4 days, with a preliminary session for tutorials. The session was based on different technical solutions for cybersecurity both from a defender and attacker perspective.

I proposed a tutorial on penetration testing and ethical hacking with the **Metasploit** framework. I set up a simple virtual lab based on **Virtual Box** with a **Kali Linux** Virtual Machine (VM) acting as attacker, and a

Metasploitable Linux VM, a **Windows XP SP3** and a **Windows 10** VM as victims to target. The picture below shows the environment.



Virtual Lab set up for the "Hacking with Metasploit" tutorial

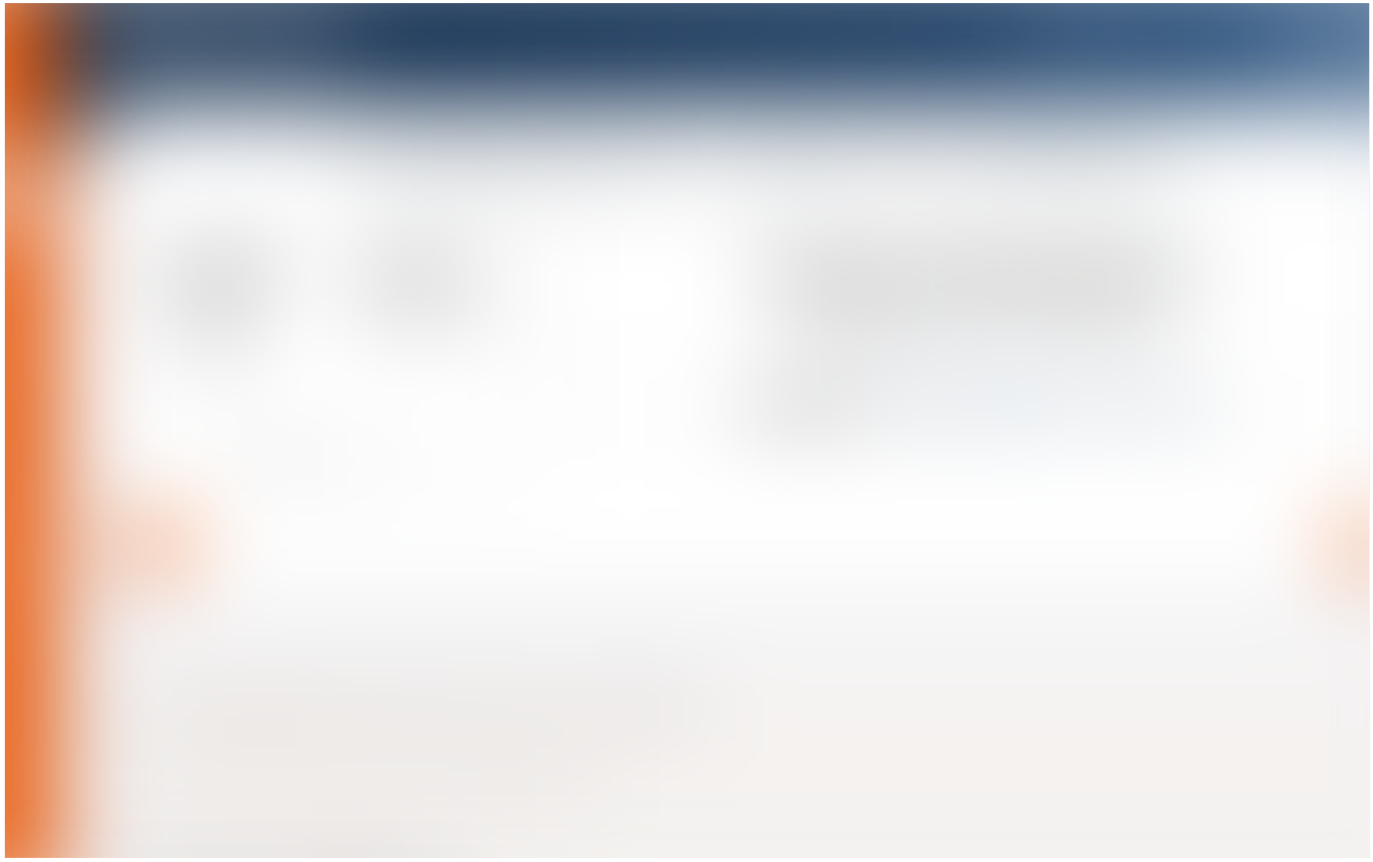
Then I started by describing the steps that an attacker needs to follow to perform an attack against a target machine, as follow:

1. **Passive Reconnaissance**
2. **Active Reconnaissance**
3. **Gaining Access**
4. **Privilege Escalation and Password Cracking**
5. **Maintaining Access**
6. **Covering Traces**

For each step I described and used some useful tools. The session was a mix between theoretical concept and practical demos.

During the first step (*Passive Reconnaissance*) I showed tools for *Open Source Intelligence* (OSINT). A first tool was the **Google Hacking Database**

(GHDB) https://www.exploit-db.com/google-hacking-database. This tool is a collaborative database of *dorks*, i.e. a collection of advanced syntax of the Google search engine to find useful open information. In the picture below, there is an example of a dork created by Kevin Randall to find txt file with information related to login and password.



Then I presented a more advanced tool for gathering information on the web, namely **Discover**. It is a script developed by Lee Baird to collect information about file, domains and IP addresses of a desired target. This tool can be combined with other tools like **Shodan** and **TheHarvester** to obtain a number of information and successfully perform the passive reconnaissance step.

In the second phase I introduced two tools for active reconnaissance, i.e. to perform port scanning and enumeration, namely **NMap** and **ZenMap**. I showed a practical example of these tools to scan the network of the virtual lab and to find ports and services opened in the three victims VMs. Then, I showed how to find vulnerabilities by using the CVE database and the collected information. In our lab, the first example shown is the **MS08–067** vulnerability of Windows XP (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067). This is a vulnerability of the *Microsoft Server Service* for remote sharing of files and printer.

To exploit such a vulnerability I moved to the step of the attack, i.e. *Gaining Access*. Here, I introduced the **Metasploit** framework, one of the most common framework for penetration testing.

Reverse Shell explained

I described how to perform an attack with Metasploit towards a vulnerable machine through the **Reverse Shell** and I introduced the Meterpreter payload. I showed a practical example where the Kali machine through Metasploit was able to exploit the vulnerability of the Windows XP machine to create a Meterpreter shell as a payload. Thus, we had an open admin shell, having so the total control of the victim, indeed we were able to access to its file system, desktop, webcam, etc.

We repeated this attack against the Metasploitable Linux machine, by exploiting the *vsftpd_234* backdoor. Again, we had the total control of the machine with admin privileges.

Then I showed as repeating the attack against the Windows 10 machine was challenging since there was not known vulnerability. Thus, I introduced *client-side attack,* which exploit social engineering for cheating an user to click on something malicious. Specifically, I showed how to create a backdoor with **Veil-Evasion** and hide it inside a pdf file by spoofing the pdf extension and a pdf icon.

Resource Hacker tool used to spoof a pdf icon

We sent the fake pdf attachment to the victim with the Windows 10 machine and prepared Metasploit to listen for incoming connection to a specific port that we specified when we created the backdoor. Once the user opened the pdf, on the Kali machine we had an open shell on the target Windows 10 machine.

Meterpreter session opened after the Windows 10 user opened the malicious pdf

However, conversely to Windows XP and Metasploitable Linux examples, the shell we opened was not with admin privileges. So I showed another module of Metasploit to simulate a Windows update to the user.

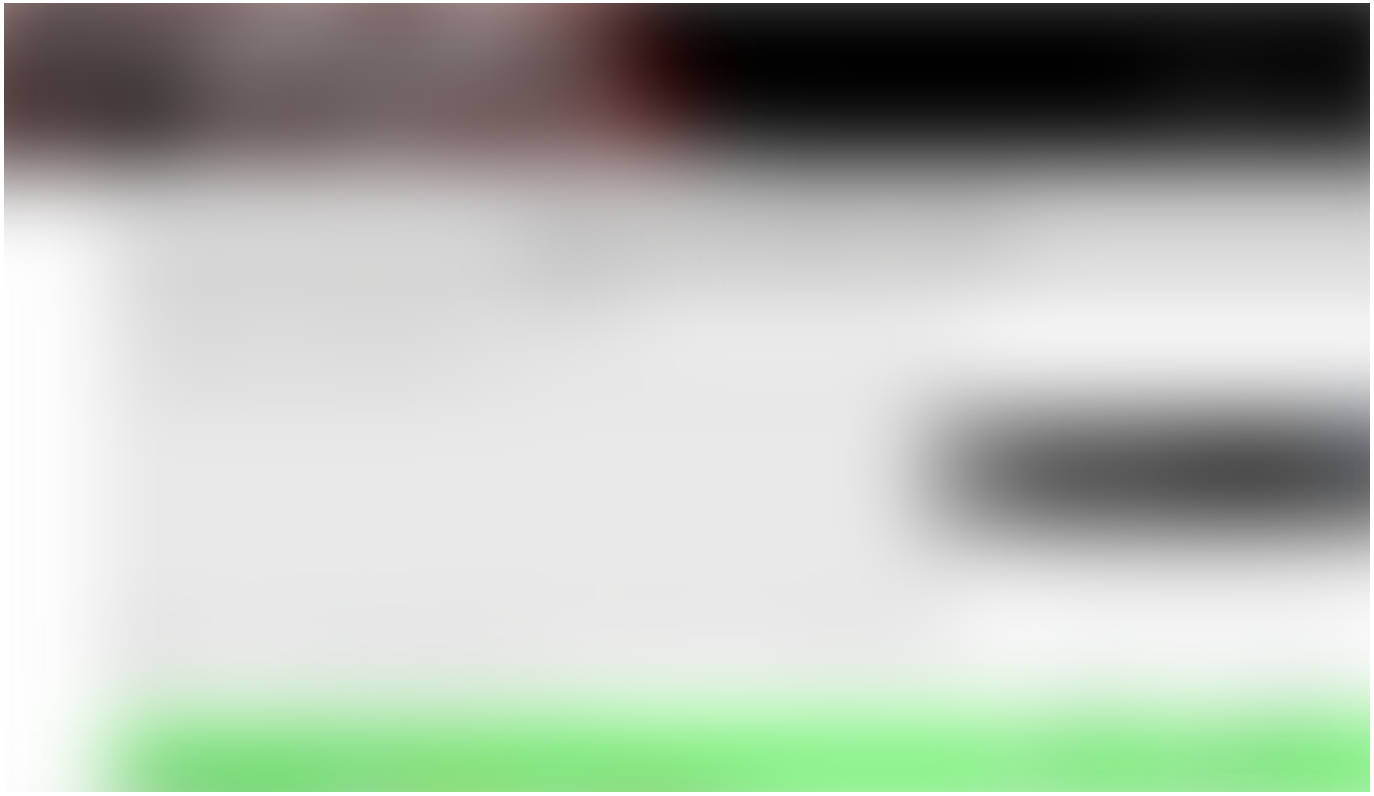
An expert user should notice this fake popup since this file to execute does not provide any signature… but how many people look at this detail?

If the user does not pay attention to this and click *yes*, is giving access to the software that launched it the privilege of administrator. In our case this software is the Meterpreter shell, thus we can escalate the privilege of the Meterpreter shell to *admin* permanently.

We also introduced different approaches for *Privilege Escalation*, for example by using a keylogger (Meterpreter Keyscan) and steal password, or using the Metasploit Hashdump to dump the password database.

Hashdump module to dump the password database of a Windows machine

The figure above shows how Hashdump can save the password database. The problem is that those are not the passwords, but the hashes of the passwords. We have to revert the hash to obtain the real password. For that scope, I showed **John The Ripper** and an online free tool, i.e., crackstation.net.



CrackStation tool to revert the hash dumped with hashdump

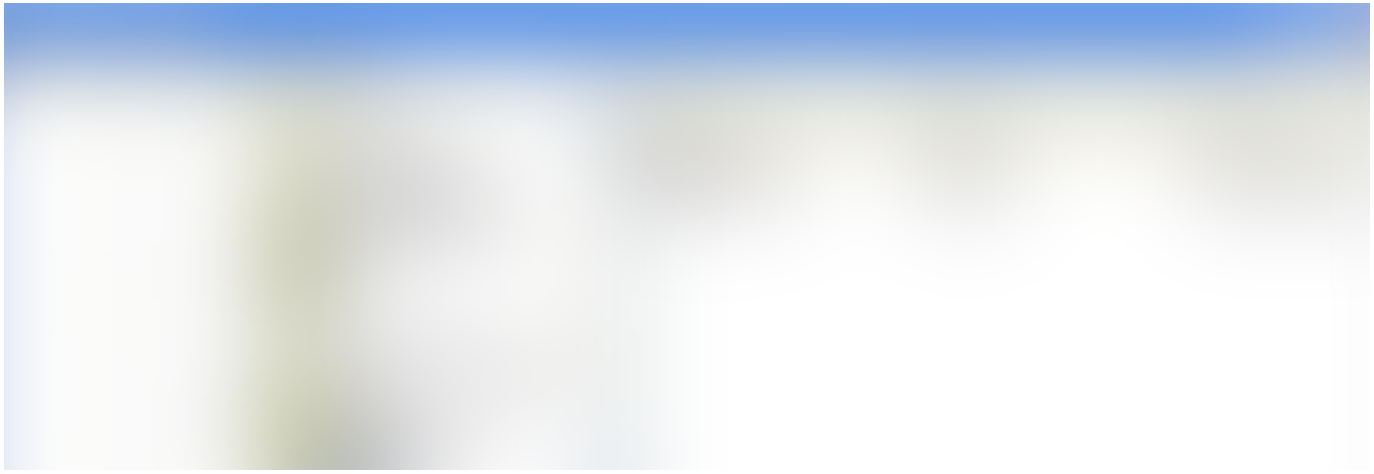
In the last part of the tutorial, I first described how to maintain a permanent access by placing a backdoor in the target machine. Figure below shows Meterpreter installing and executing the backdoor.

Metasploit installing a backdoor for permanent access

vbs script placed on the target

The backdoor is placed as a vbs script stored on the victim. This script launches an exe file.

Furthermore, it writes in the Windows registry the key in the autorun command. In that way every time the computer startup the backdoor is executed again to open again a new meterpreter session on the attacker side.



Registry key to run the backdoor at system boot

In the last section, we detailed some techniques an attacker can use to cover his trace with solutions for clearing logs, timestomping the accessed resources and use rootkit to avoid to be detected.

Finally, we had a 10 minutes session of question and answer to interact in which we discussed about some best practice that everybody must follow to minimise the cyber risk.

> *The goal of the tutorial was to give a practical overview to technical and non-technical users how simple can be to be hacked if not well protected.*

The tutorial has been highly voted on the Whova app by attendants and few companies asked for collaborations on this direction. This topic is modern and of interest of companies and public entities. I strongly believe that is a good starting point to increase the awareness of users and employees, and I

also believe that with practical examples of what can happen people can effectively learn.

Hacking | Metasploit | Kali Linux | Cybersecurity | Penetration Testing

58 claps

WRITTEN BY

Federico Lombardi

Lecturer - Cybersecurity and Blockchain Research

Follow

Cyber Security Southampton

Cyber Security Southampton Blogs

Follow

See responses (1)

More From Medium

Related reads

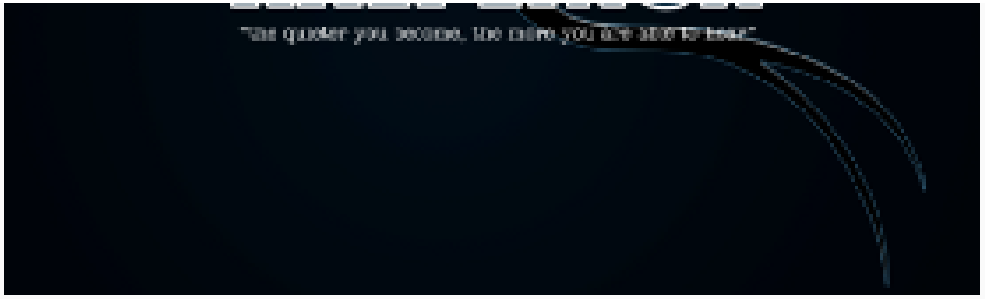
The Hitchhiker's Guide to Bug Bounty Hunting Throughout the Galaxy. v2

Nick Jenkins
Jan 30, 2018 · 9 min read

2K

Related reads

How To Install LAMP Stack on KALI Linux



Related reads

Bounty Write-up (HTB)