MAY 2020

ETHICAL HACKING

EXPLOITATION LAB

ESZTER KARAJZ

ASSESSMENT OVERVIEW

This penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge.

With the help of the Metasploit environment and a payload generator called msfvenom I create a trojan, establish reverse tcp session, dump password hashes and crack the hashes to reveal the password of the administrator.

The payload is commonly delivered to the victim's machine by the form of Social Engineering or DNS Hijacking. Once the payload reaches the destination it has to be executed.

The common examples are:

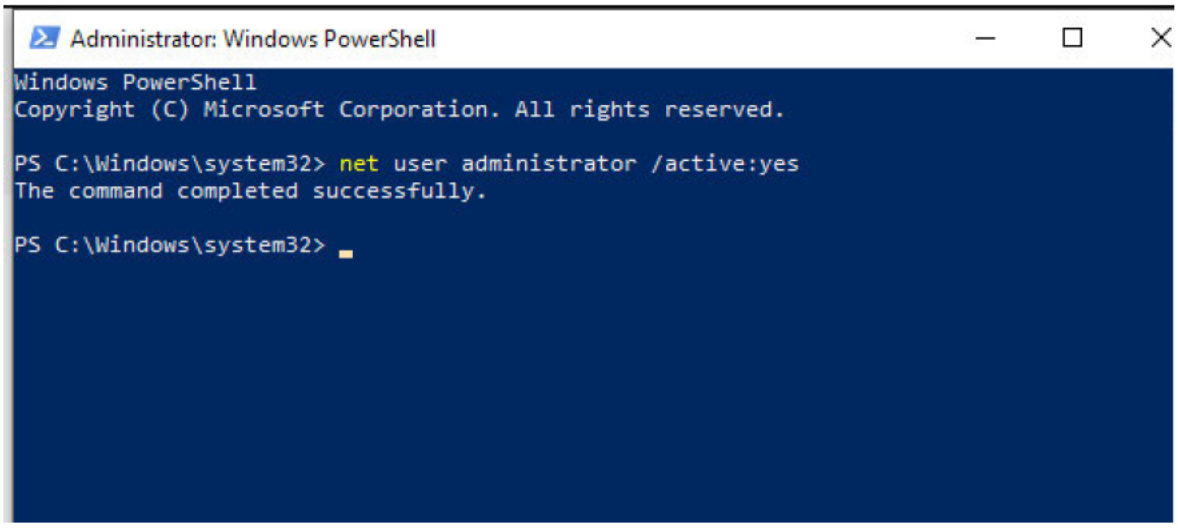
- Opening an executable file from an email attachment or downloaded from a website.
- Opening non-executable file such as pdf, jpeg or doc. In this case the payload is hidden within an image or document.

Upon successful connection the Attacker can perform data theft, monitor user's activity, run background processes and delete or modify files.

LAB SETUP

To start my lab I set up two virtual machines (later: VM). A Kali Linux VM is the attacker and a Windows 10 VM is the victim.

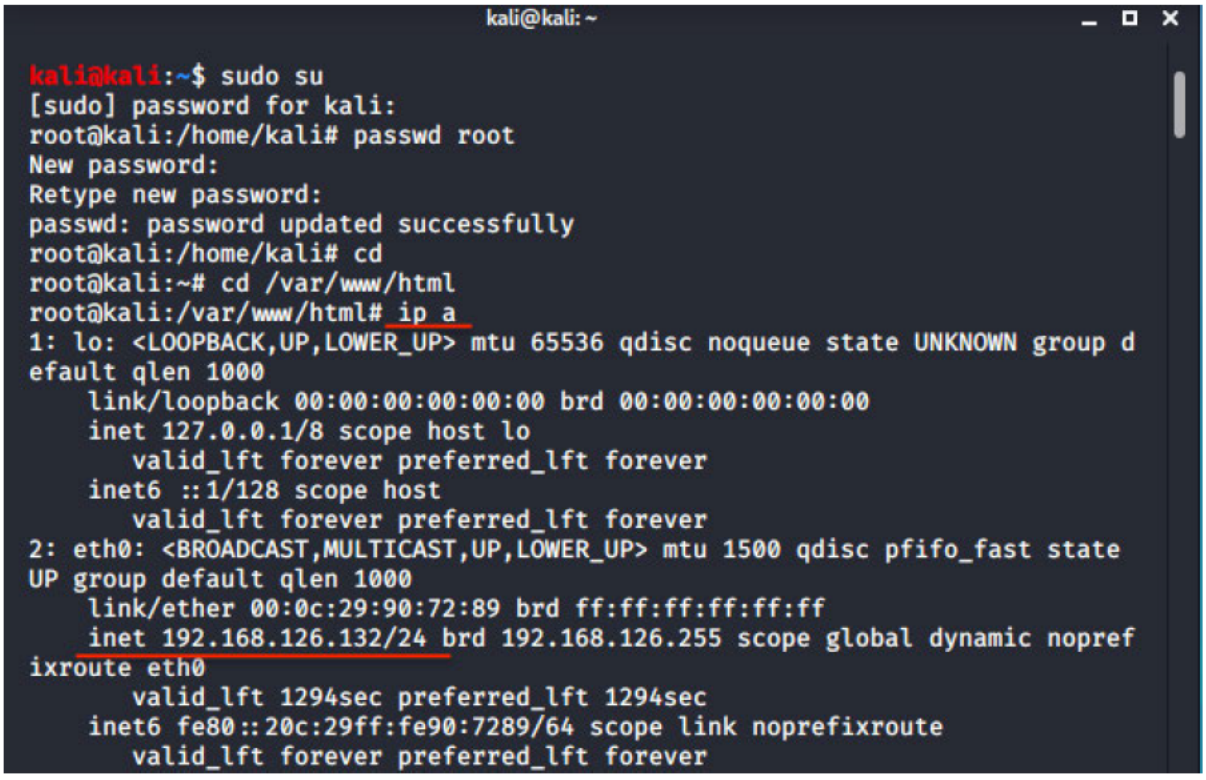
On the Windows 10 machine I open PowerShell as an Administrator and type the command 'net user administrator /active:yes' which makes me an Administrator.
I also use the 'net user Administrator + password' command to create a password for the administrator account.
After this I am able to log in to this account, so I proceed to do so.



INSTALLATION

In the Kali Linux VM I start Apache and confirm that it's working by visiting the localhost address in the browser.

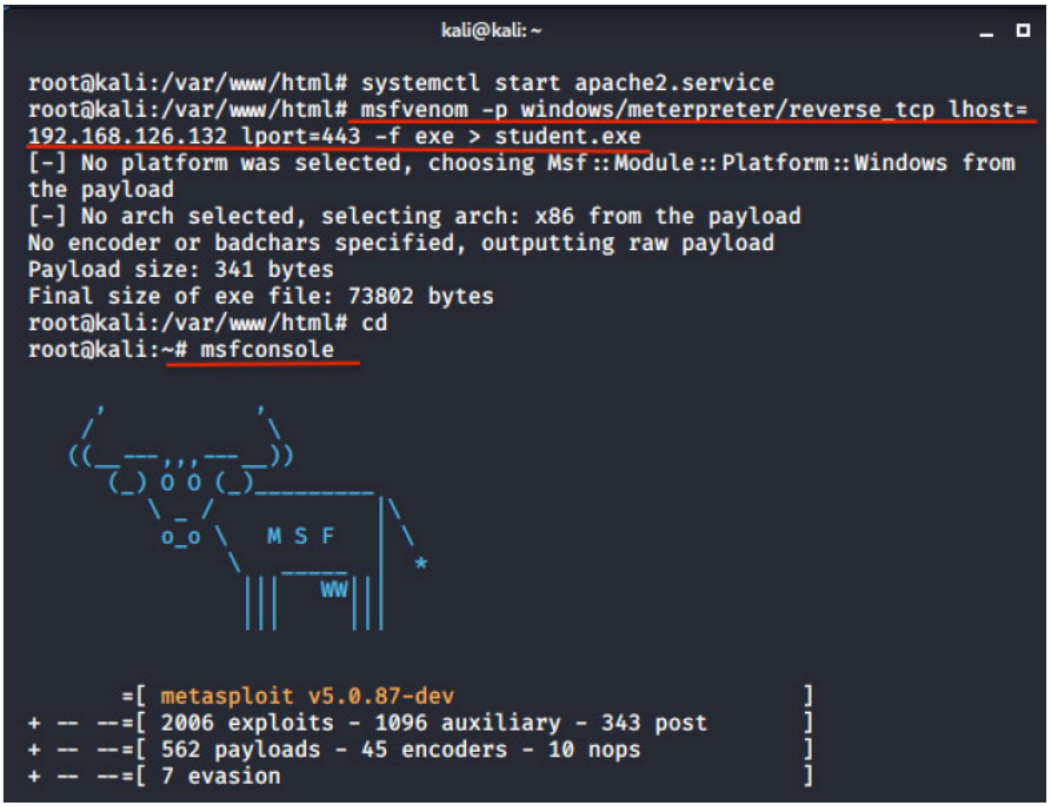
I navigate to the /var/www/html directory -which is the default location of the server- as this is where I am going to place a file called 'student.exe'.



I validate the IP address that I am using which is 192.168.126.132.

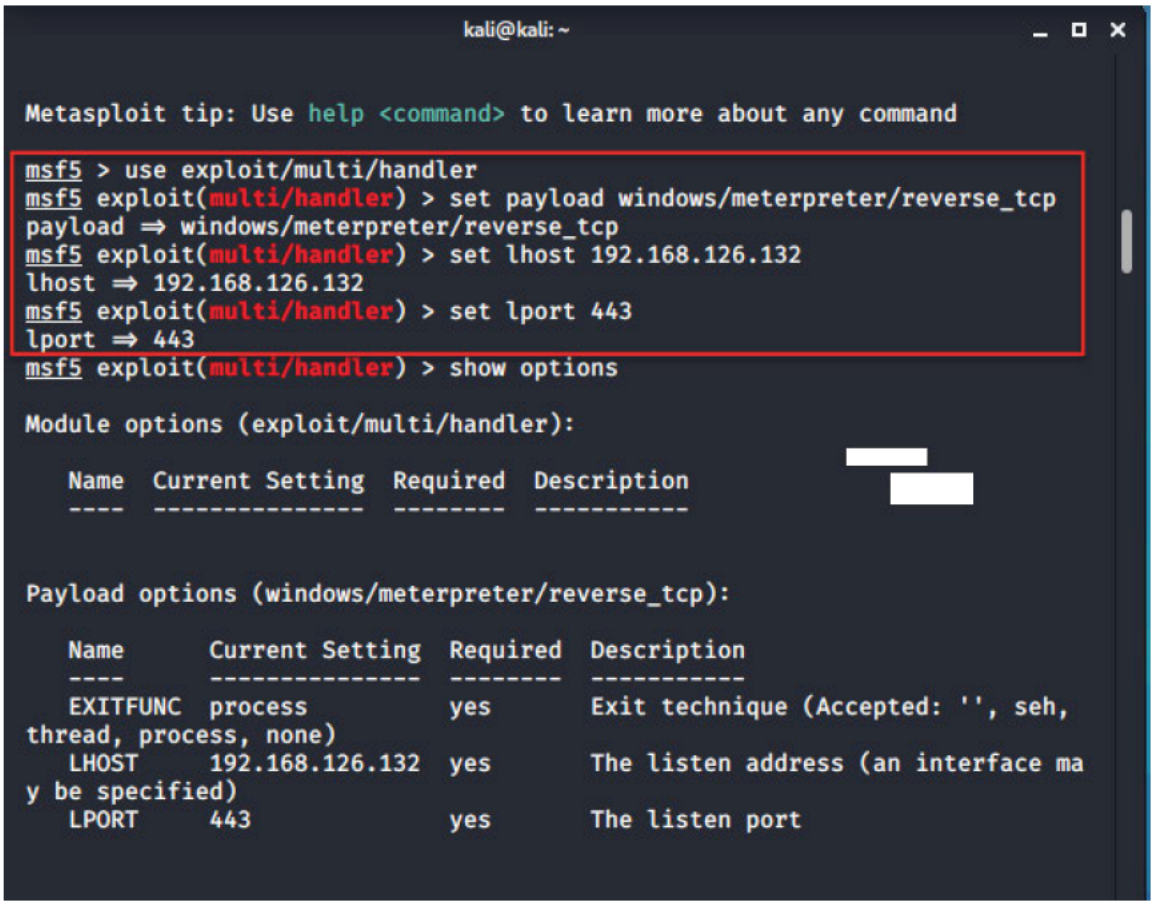
PREPARING THE PAYLOAD

I execute the command that will generate the payload hidden in the student.exe file then run the msfconsole command to start the Metasploit Framework.

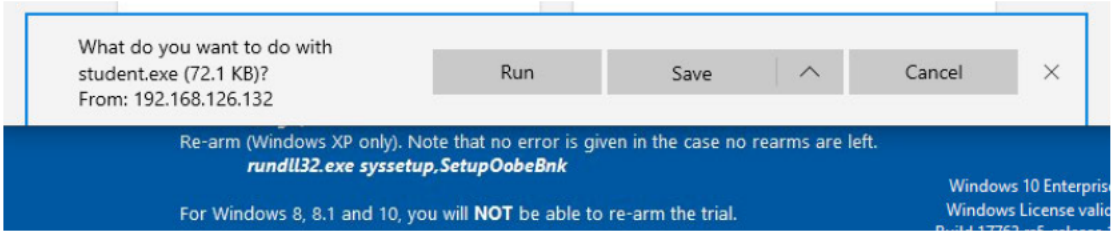


According to the official documentation "The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development."

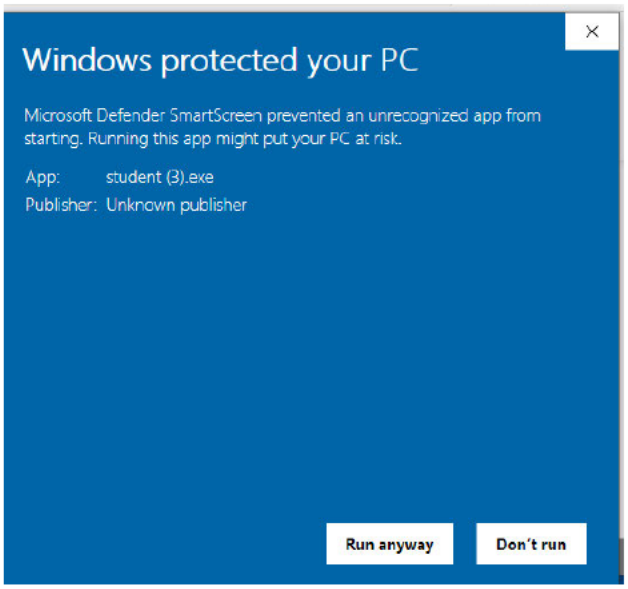
After generating the payload I use the multi handler and set the listen address to the IP address of my machine and the port to 443 which is used for web browser communication.

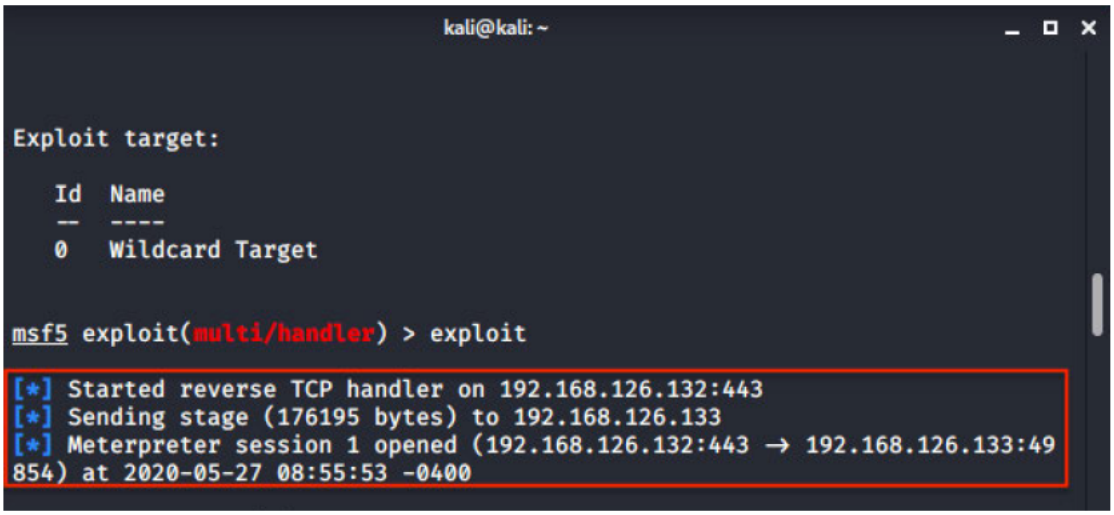


The firewall blocks incoming connections on open ports, but does not block outgoing traffic so I initiate reverse TCP connection to bypass the firewall.



The user opened the file. The payload on the Victim VM is now connected to the Attacker VM.





EXPLORING THE VICTIM MACHINE

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > migrate 3792
[*] Migrating from 2540 to 3792...
[*] Migration completed successfully.
```

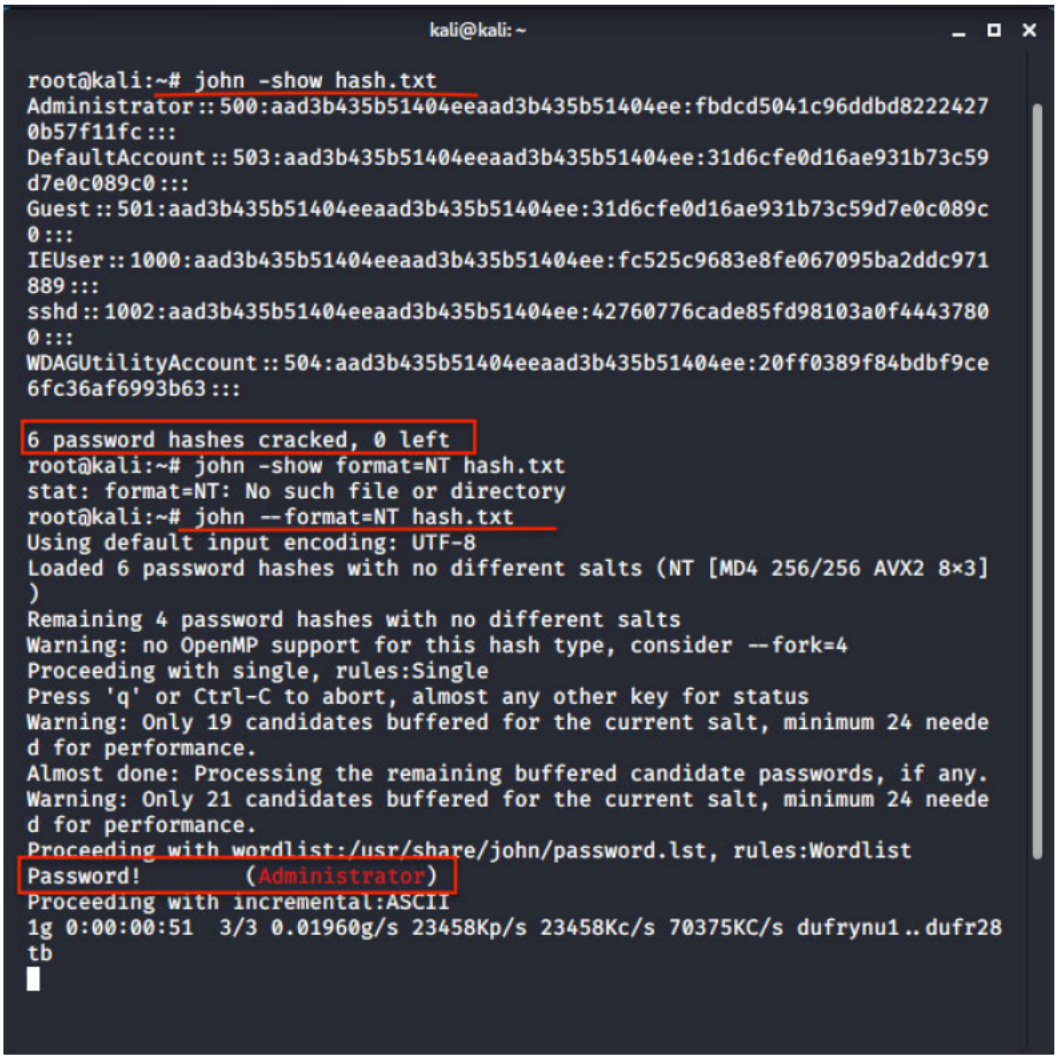
I plan to use the hashdump command to find out the password hashes. To be able to execute the command I migrate a different process that runs on a x64 architecture just like Windows 10.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fbdcd5041c96ddbd82224270
b57f11fc:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc9718
89:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6
fc36af6993b63:::
meterpreter >
```

When the migration is complete I run the hashdump command to get the hashes.

CRACKING THE WINDOWS 10 HASHES

After doing some research I decided to use John the Ripper (JtR) to crack the hashes. JtR autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match.



I create a .txt file with the 'nano hash.txt' command, copy the hashes into the file and run the commands you can see underlined. This process reveals the Administrator's password.

SECURITY WEAKNESSES

VULNERABILITIES	RECOMMENDATION
Real-time virus and threat protection was disabled.	Enabling real-time protection as it locates and stops malware from installing or running on the device.
The malicious file was opened.	Scheduling regular security awareness training for employees as they are an easy target. This can greatly reduce the cybersecurity risk of the organisation.
The administrator account uses a weak password. As the format is predictable the password can be easily discovered.	Using passwords that are long and include numbers, symbols, upper- and lowercase letters. Avoiding passwords that contain obvious personal information. Changing passwords regularly.

EXTERNAL RESOURCES

- https://metasploit.help.rapid7.com/docs/msf-overview
- Heath Adams: Practical Ethical Hacking - The Complete Course (Udemy)
- https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/breaking-password-security/breaking-windows-passwords/#gref
- https://www.varonis.com/blog/john-the-ripper/
- https://www.top-password.com/blog/crack-windows-password-with-john-the-ripper/