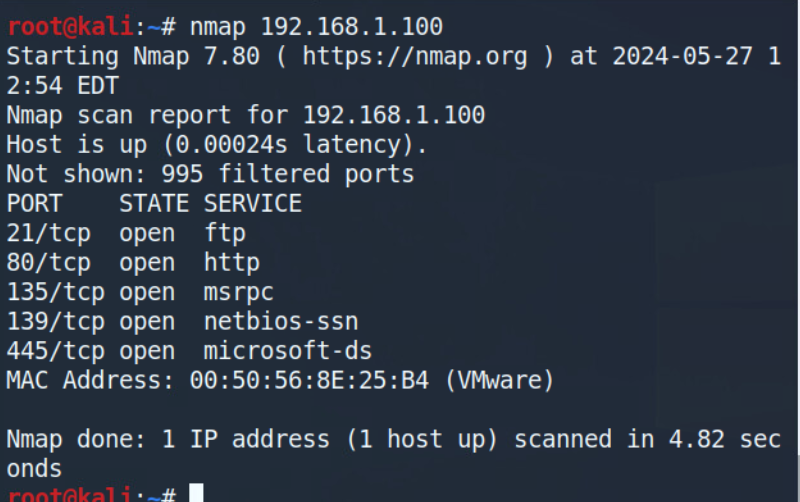
reIn this lab, I am exploiting a Windows Machine with Metasploit by using a vulnerability found with Nmap. I will then use this knowledge to harden the system so it doesn’t happen.

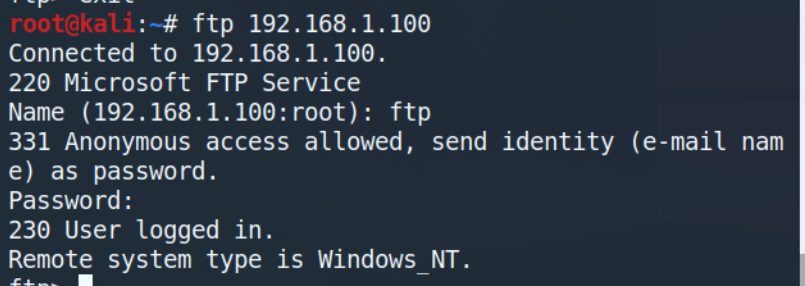
### **Open Ports**

I am using a Kali Linux system. I can ping the other Windows System in the network. I also use nmap to scan the system for any open ports.

#### **FTP**

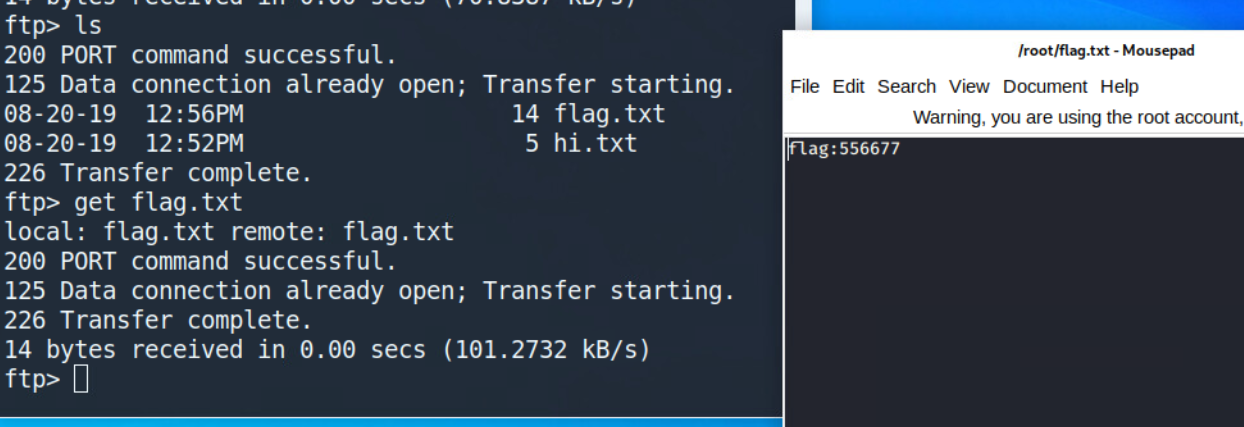


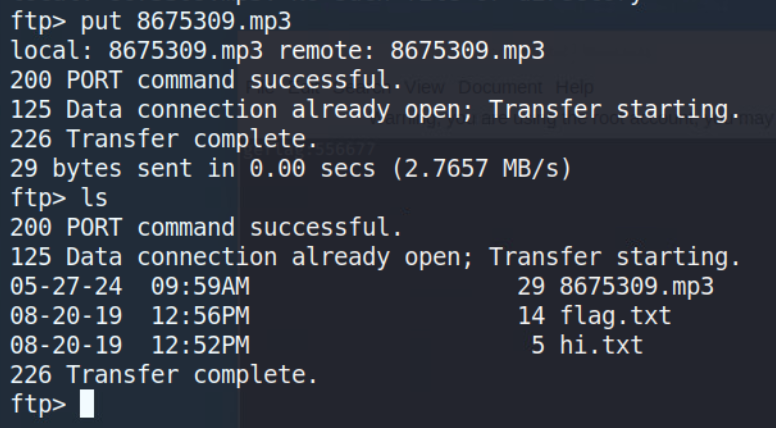
FTP sends data in clear text making it vulnerable, making it a good target to exploit. Additionally, anonymous users are sometimes allowed to download and even upload files to a server. If anonymous access is allowed, then putting “ftp” in the user and any password will be accepted no matter what. I don’t put anything in the password, only pressing enter, and it still goes through.



Now that I have logged in anonymously, I can view what files I can download from the server.

**‘get flag.txt’** to download the file named flag.txt in plain text as FTP is not secure.

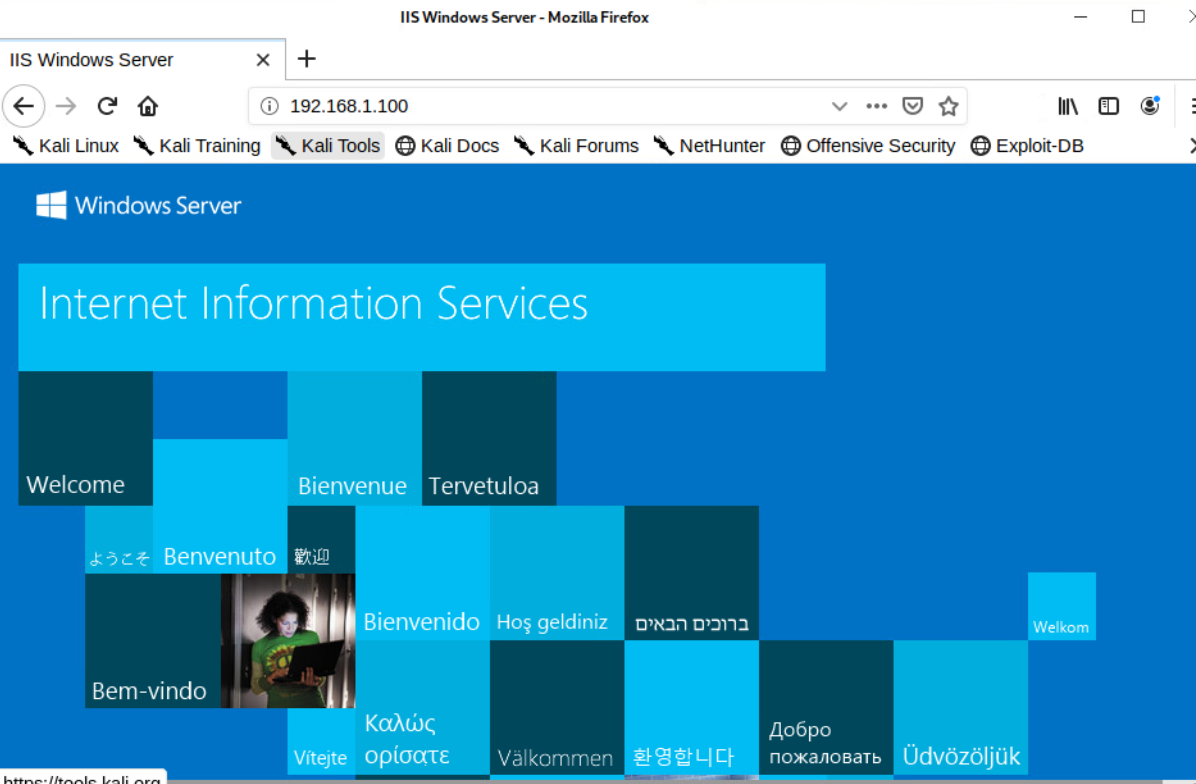




**‘put 8675309.mp3’** to upload the mp3 file to the server. This is a critical threat allowing people to store files that should not be there.

#### HTTP

In the Nmap scan, the HTTP port was also shown to be open. I can type ‘192.168.1.100’ in the URL bar of a web browser to see if a website has been set up for the company. It seems to be the default IIS web page, so it has not been configured.

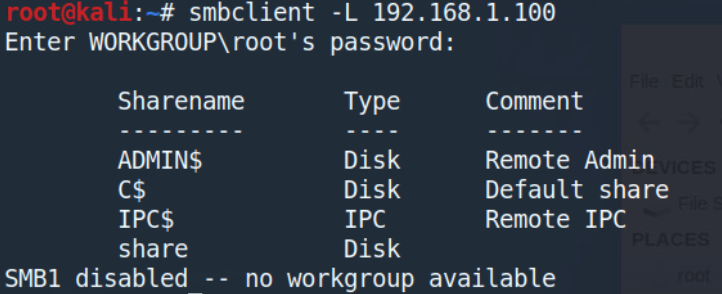


#### SMB

The Nmap scan also showed port 445 open. I am completely unfamiliar with SMB, so I am following the lab closely.

**‘smb -L 192.168.1.100’** to list the shares on the system

When prompted for the password, I was able to just hit enter and then I had access.



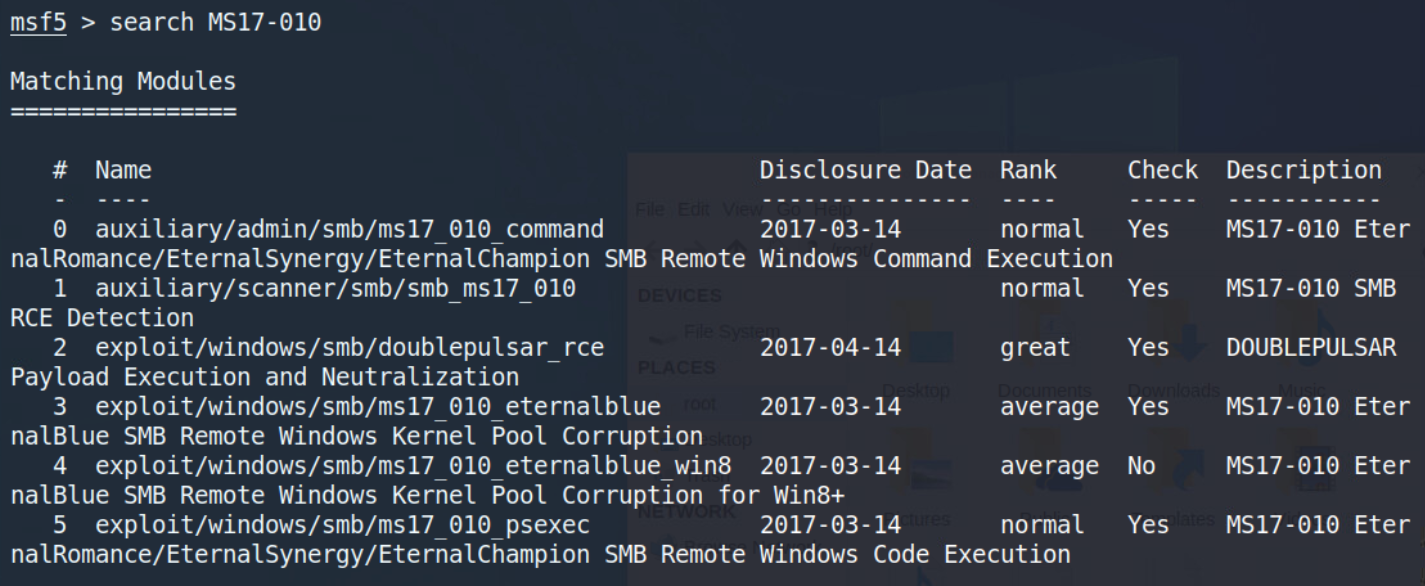
There is a critical 2016 SMB Windows Server vulnerability designated as MS17-010, this is what will be used to exploit the machine.

### **Exploiting the Machine**

**‘msfdb init’** to initialize a metasploit database

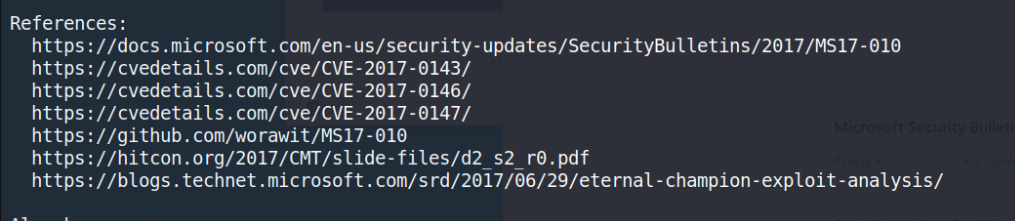
**‘msfconsole’** to initialize metasploit

**‘search MS17-010’** to search for exploits

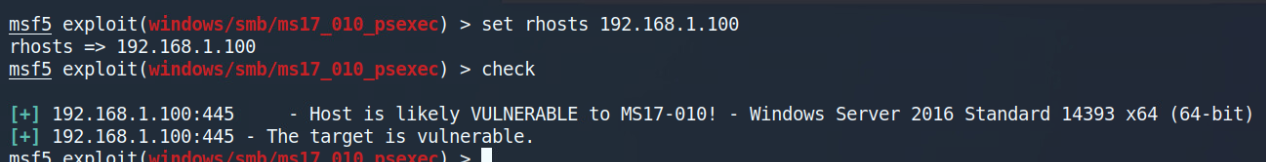


(5) to select the ms17\_010\_psexec exploit

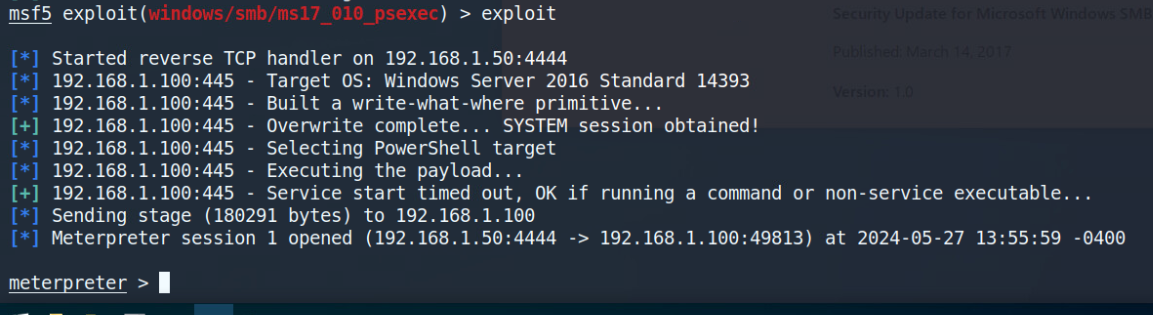
With this exploit selected, I can type **‘info’** to get relevant information on the exploit, especially finding references on the exploit which can then help me secure this system from the exploit later on.



Back to exploiting the machine, after setting the remote host ‘RHOSTS’ to the target IP, I can use **‘check’** to tell metasploit to see if the system is vulnerable to the exploit



It seems I don’t need to set ‘LHOST’ so I can just ‘exploit’. A meterpreter shell opens up.

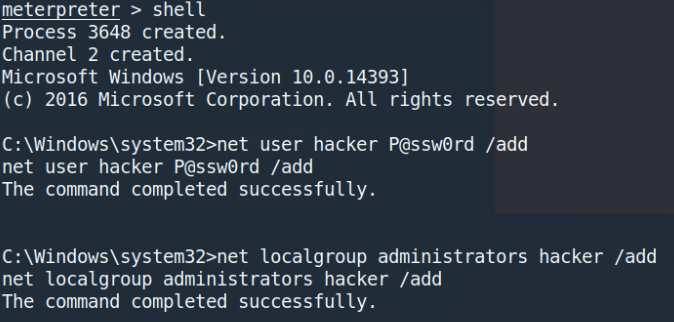


‘shell’ to enter the Windows command prompt of the system. This could be more useful to those who are more comfortable working in command prompt as the commands differ from meterpreter and cmd. There may also be additional functionality, but I don't even know the full scope of meterpreter yet

WIthin command prompt, I can create a new user and escalate that user to have admin permissions

`net user hacker P@ssw0rd /add`

`net localgroup administrators hacker /add`

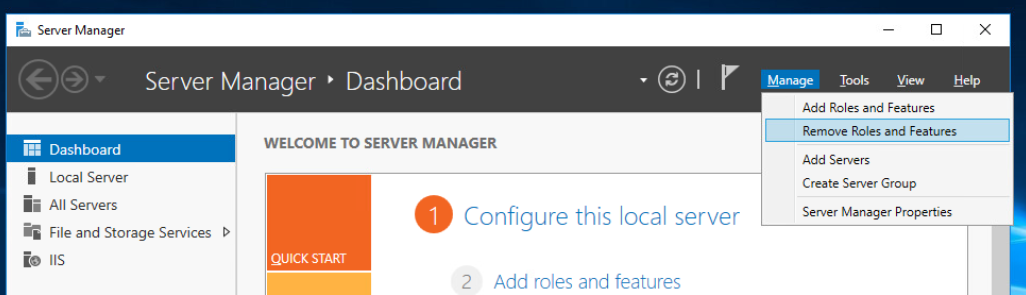


### **Hardening the Machine**

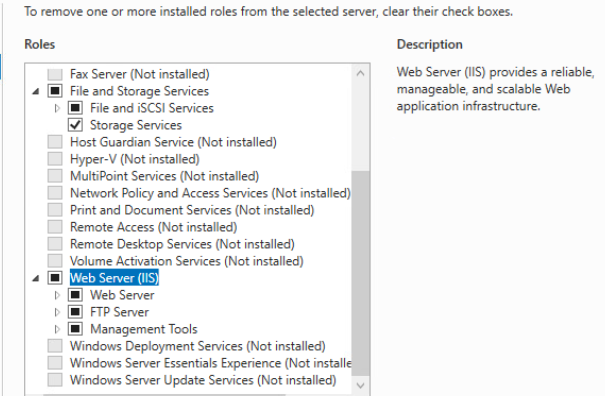
Now working on the Windows machine that was just attacked.

When logging in, a “Server Manager” window opened up.

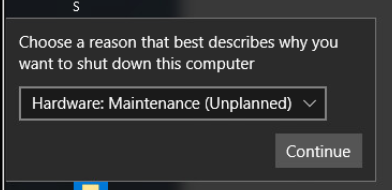
#### FTP and HTTP

Manage → Remove Roles and Features

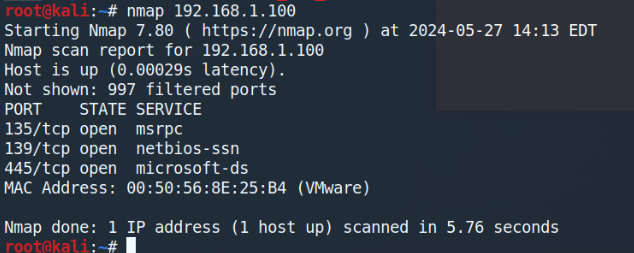
In this menu, I can see all the roles that are enabled



From here, I can remove all the roles related to the Web Server. The website is not configured at all and it seems to not be needed as it was not being used. This also removes the FTP server from being active, removing that vulnerability. After that, I restarted the computer.



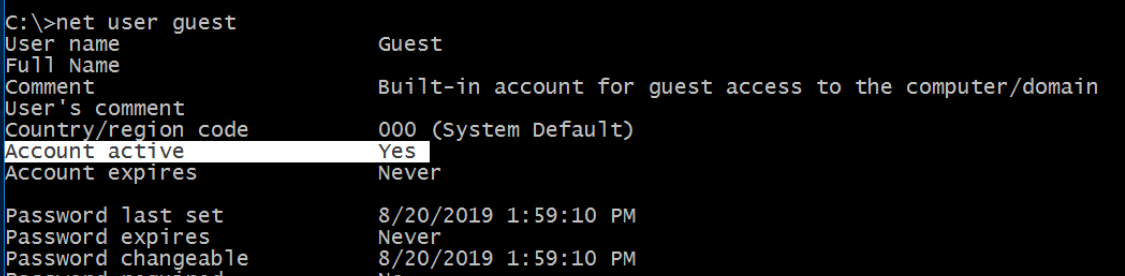
Now, when going back to the Kali machine and scanning the Windows machine with Nmap, the HTTP and FTP ports are no longer showing up as open.



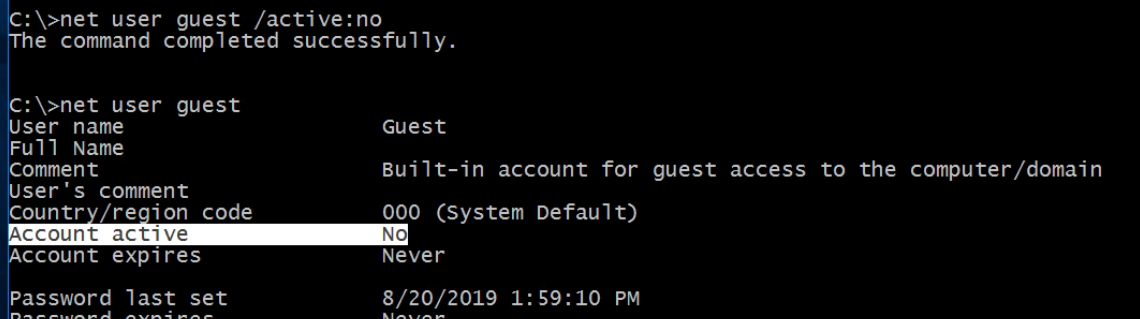
The SMB vulnerability is still up, at this point, so now I will secure the system from that.

#### SMB

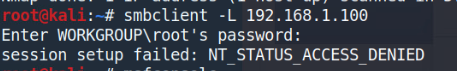
Going back to the Windows machine, the guest user for the system is active which is allowing attackers to browse shares on the machine, as well as allowing the MS17-010 exploit to work.



**‘net user guest /active:no’** to disable the guest account

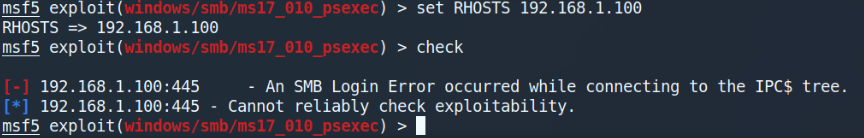


Now back on the Kali machine, I can no longer enumerate the shares on the system as I can’t get access without the correct password.

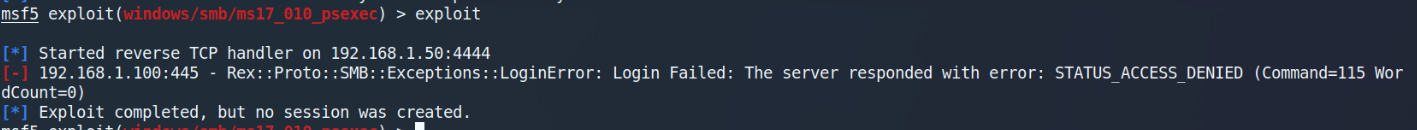


Additionally, I run into problems when I attempt to exploit the machine again in the metasploit console.

**‘check’** to see the vulnerability of the machine to the exploit shows an error due to “an SMB Login Error”



**‘exploit’** to run the exploit, I can no longer create a session with the machine



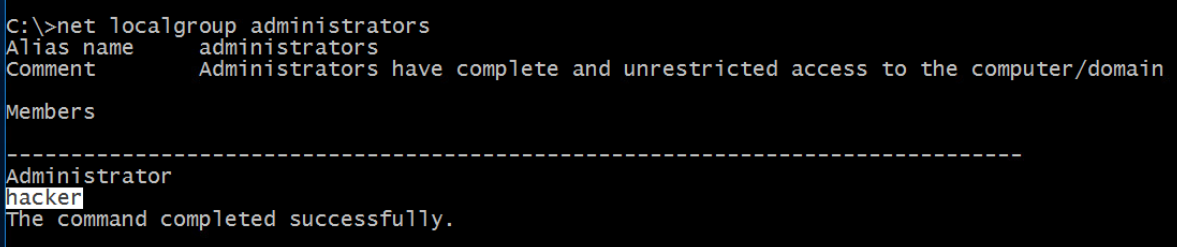
I find it amazing how something as simple as disabling the guest account can completely prevent this attack.

#### Cleaning Up

Now that the vulnerability is closed, I can clean up the damage done by the Kali machine

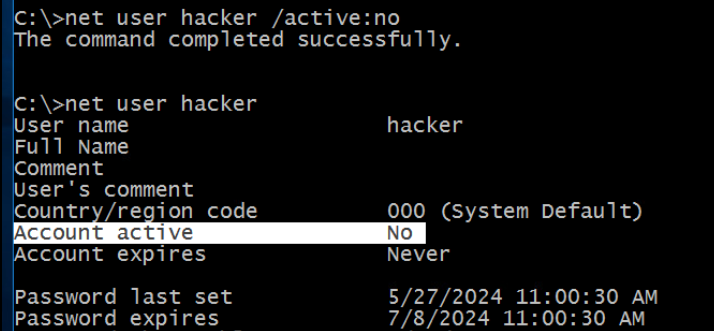
On the Windows machine, I can view users with administrator permissions

**‘net localgroup administrators’** to view users in the administrator group



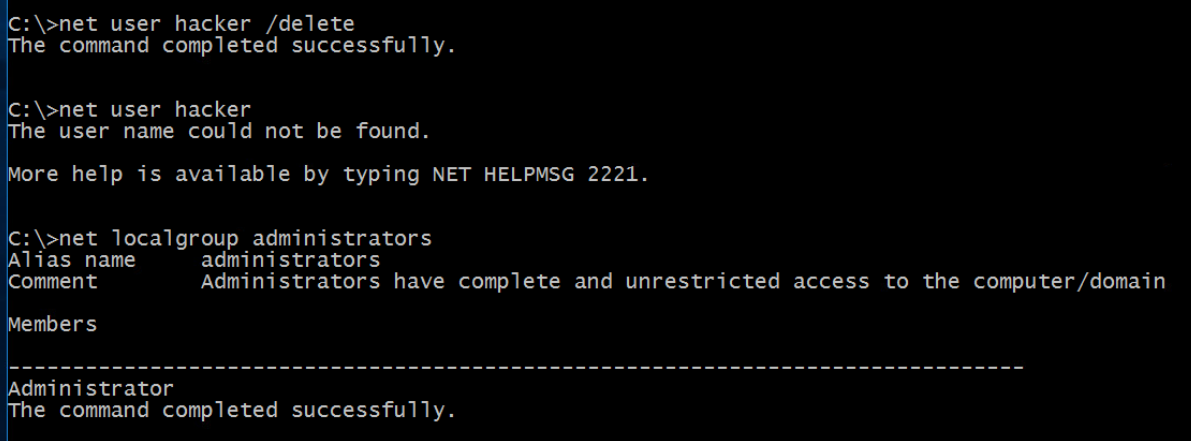
I see that there is an unauthorized user with administrator permissions, so I can disable the account

**‘net user hacker /active:no’** to disable the user named hacker



Now I can remove the account entirely from the system

‘**net user hacker /delete’** to delete the user named hacker



### Skills

Windows Hardening

Nmap

Metasploit

Windows

Command Prompt

Kali Linux

Linux Terminal

Meterpreter

### What to Learn More About (just notes for me)

What SMB is, what are shares, why are they significant

Different services

Famous exploits