Starting with Nmap scan to see what ports are open so that we can determine what open port we can attack.

$ nmap -sC -sV -v -oN Active-Initial 10.10.10.100

With this command we will enumerate the machine with nmap scripts to find if there are any vulnerabilities (-sC), we will enumerate the version of the services running on those ports (-sV), we want nmap to show us the output of everything it's doing (-v) and lastly we want nmap to output the scan in a file, so that we can reference to any port that was caught open by the program (-oN).

We can see a lot of ports were found. The next thing we have to do is to check what services are running on those ports.

We can see that we have some interesting ports open:

Port 389 - ldap - Microsoft Windows Active Directory LDAP (Domain: active.htb ... )

Port 3268 - ldap -

Port 135 - msrpc - Windows RPC

Port 139 - netbios-ssn - Windows netbios-ssn

Since the machine's name is "Active" and we saw that we have ports 389 & 3268 Ms Windows Active Directory open, we can say that we have to deal with Active Directory later on. Now smb is open, so starting with and trying to find exploits was the first thing I opted for. Trying some of the exploits from Metasploit such as the MS17\_010\_Eternalblue exploit would not work. What I decided to do next was to run a Nessus scan to check for some vulnerabilities that I couldn't think about. Nessus found a vulnerability that can be exploited for the SMB service.

Now this is something interesting. By doing a bit of a research about NULL session vulnerability in SMB I found out that this vulnerability allows a connection to be made without supplying a valid user or password. Now lets see how to exploit it. Searching in google I found a tool called "nullinux" that will help me do some enumeration on the SMB service.

Link: https://github.com/m8r0wn/nullinux

I downloaded the program and set it up.

$ git clone https://github.com/m8r0wn/nullinux

$ cd nullinux

$ ./setup.sh

$ ./nullinux.py -h

Let's see how to run the program.

Looking at the options, there is "-a, -all" to enumerate users and shares and "-v" for verbose output.

Next I ran the program.

$ ./nullinux.py -a -v 10.10.10.100

Lets check the output !

Great ! I found some shares that I can try log in use a null session. I skipped the first two (ADMIN$ & C$) since these shares won't be exploitable by the null session vulnerability.

There two interesting shares that I can try: Replication & Users

So to try the null session exploit, there is a tool that we can rely on thats pre-installed in Kali: smbclient. I tried to connect to Replication first and it was successful... Let's enumerate !

$ smbclient //10.10.10.100/Replication

After enumerating the shared folder I found an interesting file called "Groups.xml" and I downloaded it to check what's inside it.

Perfect ! It seems I found a user and a password hash ! Trying to identify the hash with hash-identifier didn't help, so I did a research about what type of hash does windows store in Group Policy. It turned out to be AES-32 which is technically AES-256. So I search how to decrypt cpassword and there is a tool that comes with Kali: "gpp-decrypt". Let's decrypt that password !

$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

An alternative to the gpp-decrypt tool is this one gpprefdecrypt.py. Now I have the password, let's try to login with that user.

$ smbclient //10.10.10.100/Users -U SVC\_TGS

I used the shared folder Users because we have in it nullinux output and this is second shared folder that caught my eye in the enumeration process. After I ran the command I got access to the machine and I was able to get the flag for user SVC\_TGS.

Now came the part when I spent around 2 hours looking online and asking a great person about the Kerberos service and what possible ways I can go for to escalate the privileges and get Administrator.

Kudos to : Khr0n0s ( an amazing person ) Check him out !

I had to read about Kerberos to understand what it is used for and what does it do. Well in a nutshell Kerberos is an authentication protocol used in all of the operating systems (FreeBSD, Unix, Linux, Windows, etc...), it uses tickets to authenticate users, it does not store passwords locally but instead it caches them, it involves 3rd Party programs and has a built-in symmetric-key cryptography. I suggest to all who read this to read about Kerberos, Kerberoasting and Active Directory. That way you will get an idea how they work which is the key to success !

After searching for ways to privilege escalate from SVC\_TGS, I found a tool called ImPacket and it can be downloaded from GitHub. I read about the separate scripts and their functionality and what I had to do was to use GetUserSPNs.py to get the Service Principal Names which will be requested with user SVC\_TGS. Since we have the Ticket Granting Server (SVC\_TGS) we can use it to request the SPN for Administrator and get the hash so we can crack it !

In ImPacket, there is a python script GetUserSPNs.py that will do this for us.

$ GetUserSPNs.py -request-user Administrator 10.10.10.100/SVC\_TGS:GPPstillStandingStrong2k18

This issues was annoying and after 20 minutes of struggling to fix it I thought to my self. "Hmmm, why don't I add active.htb into the /etc/hosts file and see what happens then". Luckily this helped to resolve the issue. I now just had to change the IP with the domain (active.htb)

$ GetUserSPNs.py -request-user Administrator active.htb/SVC\_TGS:GPPstillStandingStrong2k18

Yeahhh ! Got the hash ! The last thing I needed to do is to crack the password with hashcat. I didn't needed to do any converting of the hash so that hashcat can crack it because the python script already did that for me.

Fire up hashcat !

Linux:

$ hashcat -a 0 -m 13100 <path\_to\_hash>/Output.hash /usr/share/wordlists/rockyou.txt "use --force if you don't have GPU"

Windows:

$ hashcat64.exe -a 0 -m 13100 Output.hash rockyou.txt

I did the cracking part on my Windows machine because I'm using VMware Fusion to hack the machine, so hashcat didn't work for me on the VM.

Let's check the result now !

Awesome ! Got the password for Administrator -> Ticketmaster1968 ! Now lets connect to Administrator using smbclient.

Now the last thing to do is to get the root flag ! That's how to the Active from HackTheBox !